Conheça os benefícios da rede multicloud com Cisco Cloud ACI

Rafael Guerra
Engenheiro de Sistemas
Cloud Infrastructure and Software Group

01 Desafios atuais

02 Conhecendo Cloud ACI

03 Casos de uso

04 Demo Multicloud
Terraform e Nexus Dashboard

Desafios atuais

Como vocês está lidando com as necessidade de rede

A rede hoje é complexa

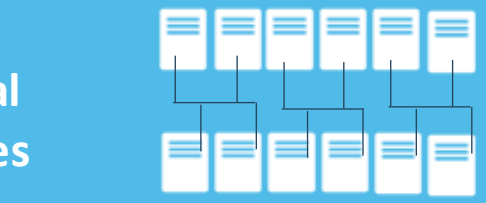
Cloud Architect
AWS, Azure, Google, IBM

Cloud Networking

Container networking

Virtual Switches

Physical Switches



Platform Admin/Developer
Kubernetes, Openshift, Cloud Foundry

VMWare Admin
VCenter

Hyper-V Admin
SCVMM

KVM Admin
RedHat (RHEV-M)/Openstack (Horizon)

Network Admin
Network Console (CLI)

Quint@s Quinze

O problema

Risk
$6T in security damages by 2021

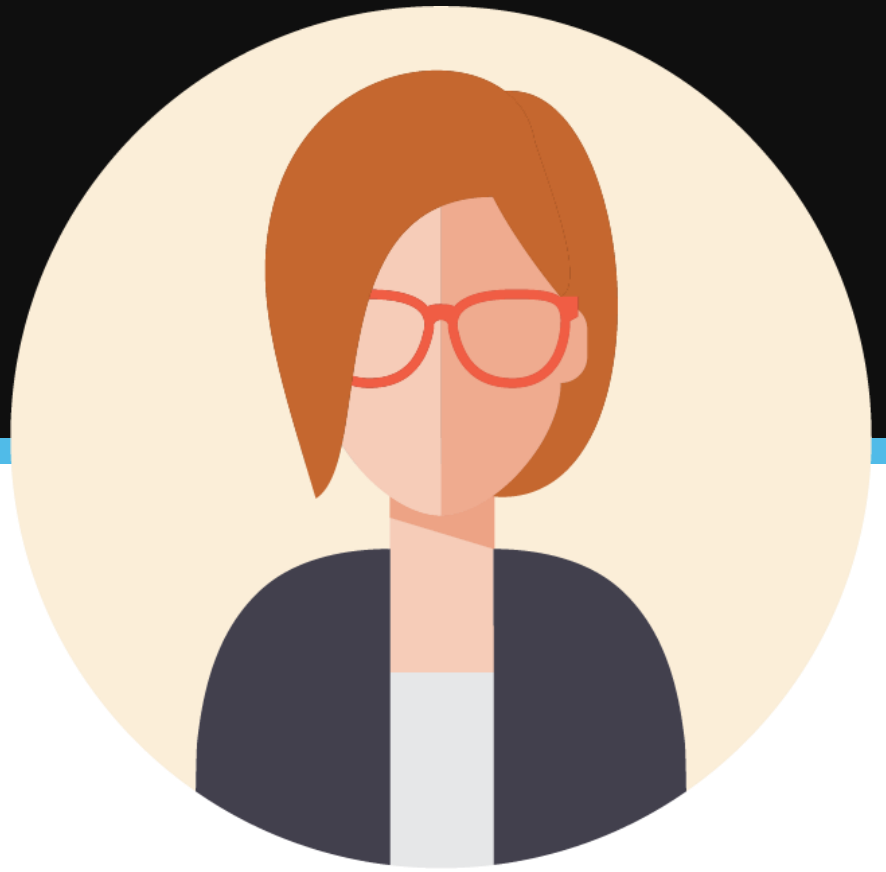
Time-to-Market
Innovate or disappear

Downtime
$5600/min

Source: Gartner & CyberSecurity Ventures

Quint@s Quinze

Há necessidade de Administradores de rede na nuvem?



Quint@s Quinze

O conhecimento de rede é fundamental na nuvem

Internet access & DNS

Segmentation & Policy

Subnets & IP Addressing

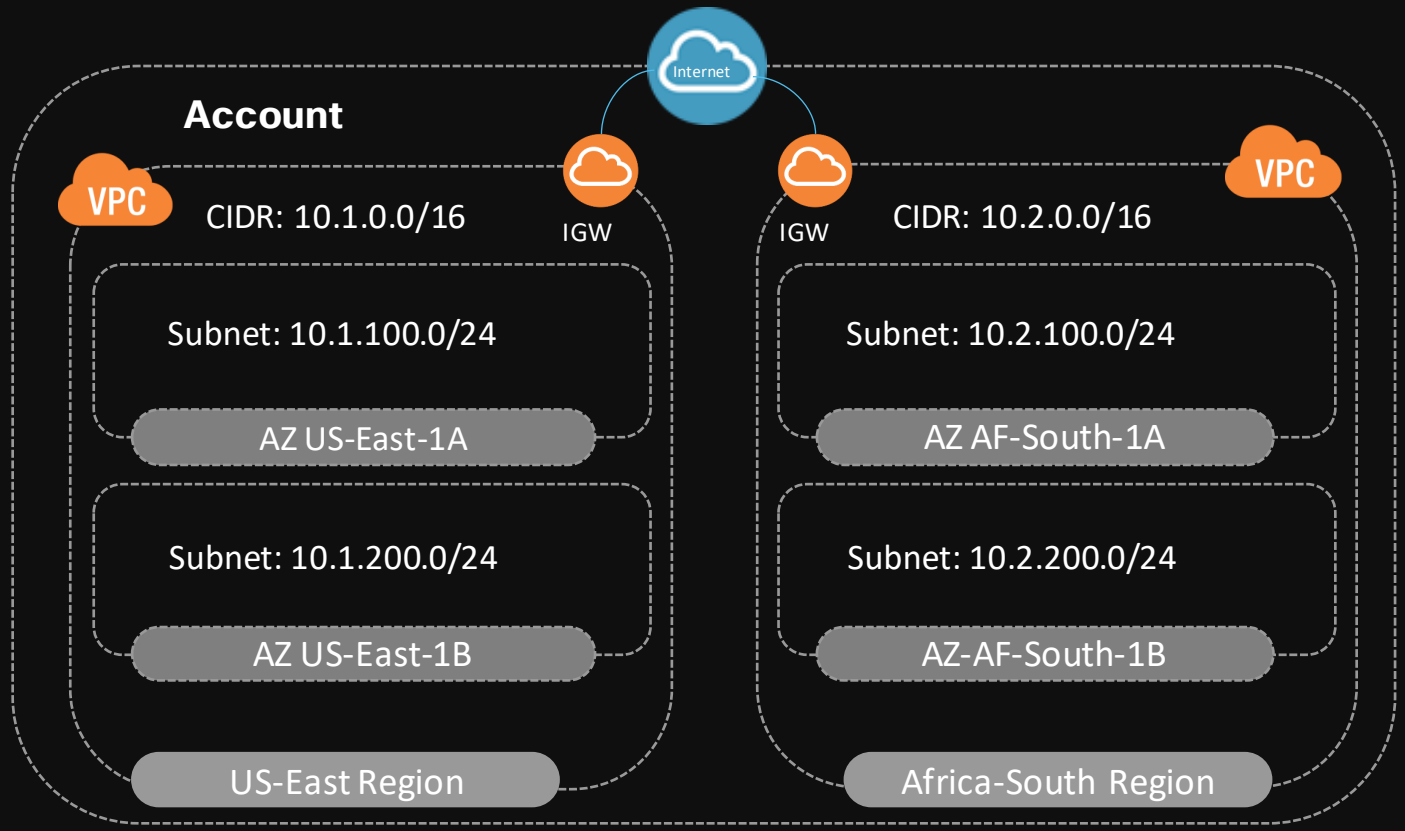
High-Availability Designs

Cloud Interconnect

VPNs, NAT & L4-L7

Quint@s Quinze

Cloud Networking: AWS



- VPCs are equivalent to VRFs
- Default VPCs are pre-configured*
- CIDR blocks created per VPC
- VPCs connect to Internet via IGWs
- Subnets derived from CIDR blocks
- Subnets are private (default) or public

Cloud Provider

Services

aws

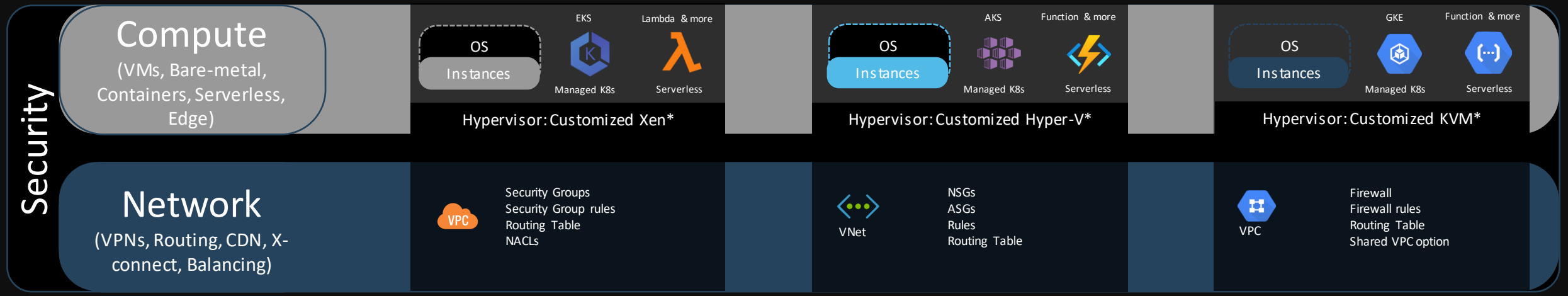
Quint@s Quinze

Cloud Networking Services

L3-based forwarding (No L2)

Broadcast traffic not supported

Multicast traffic is not supported/limited



Cloud Provider Services

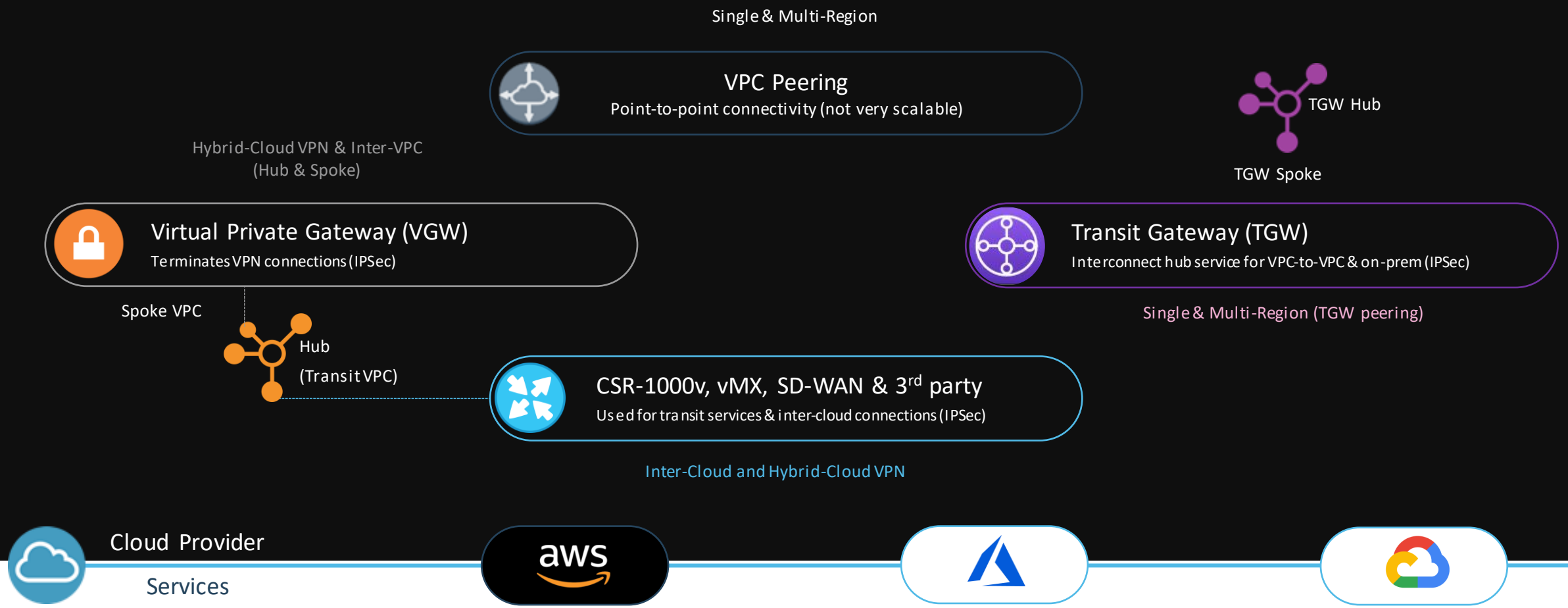
aws

* Cloud Provider's hypervisor does not allow/require any configuration

Quint@s Quinze

Cloud Networking: AWS

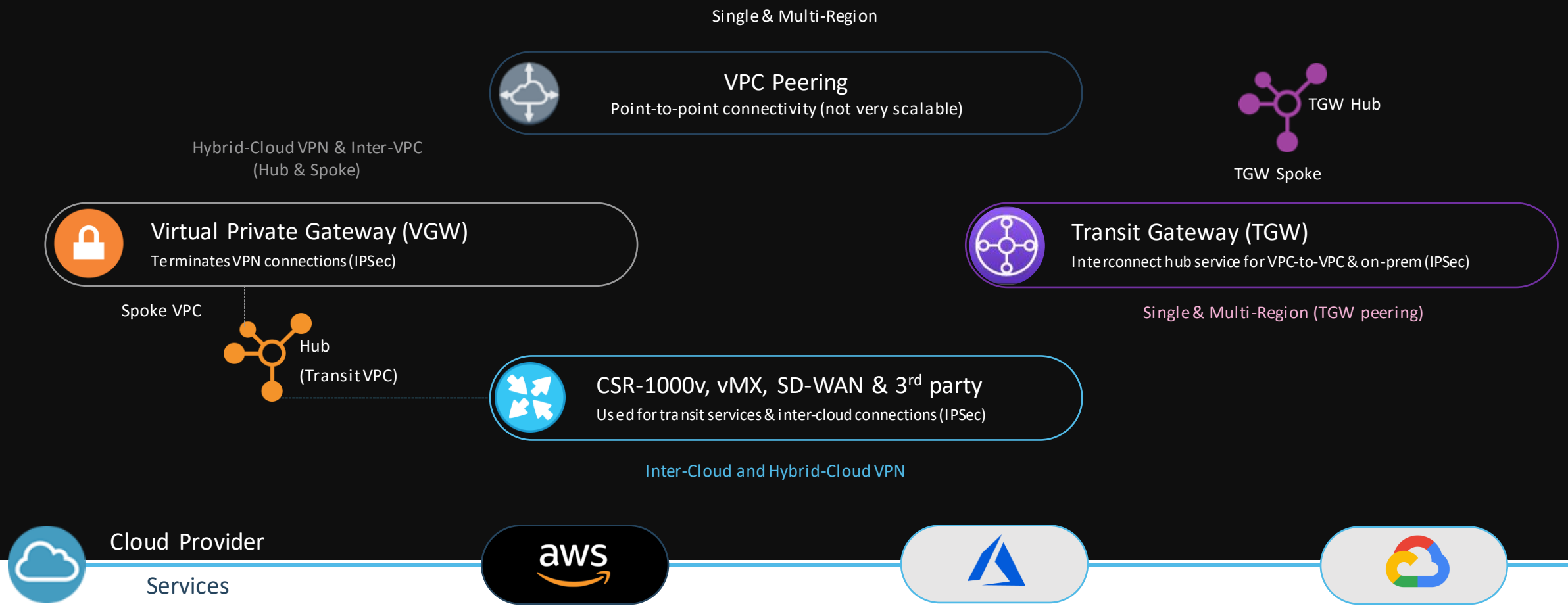
Inter VPC, Inter Region & Inter Cloud Connectivity Options



Quint@s Quinze

Cloud Networking: AWS

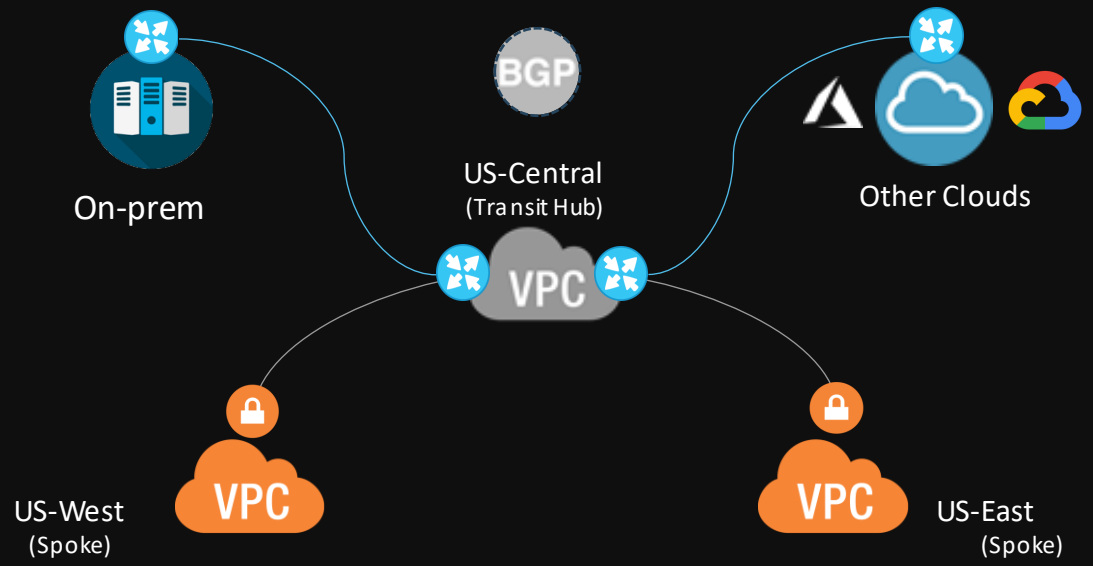
Inter VPC, Inter Region & Inter Cloud Connectivity Options



Quint@s Quinze

Cloud Networking: AWS

Hub & Spoke – VGW + CSR1Kv



Transit VPC Architecture
(single region/multi-region)

Inter VPC, Inter Region & Inter Cloud
connectivity options

Virtual Private Gateway (VGW)
Terminates VPN connections (IPSec)

CSR-1000v & 3rd party
Used for transit services & inter-cloud connections (IPSec)

1.25Gbps per Tunnel | CSR-1kv management & encryption

Cloud Provider Services

aws

Quint@s Quinze

Cloud Networking: AWS

Inter VPC, Inter Region & Inter Cloud Connectivity Options

Single & Multi-Region

VPC Peering
Point-to-point connectivity (not very scalable)

TGW Hub

TGW Spoke

Hybrid-Cloud VPN & Inter-VPC
(Hub & Spoke)

Virtual Private Gateway (VGW)
Terminates VPN connections (IPSec)

Transit Gateway (TGW)
Interconnect hub service for VPC-to-VPC & on-prem (IPSec)

Single & Multi-Region (TGW peering)

Spoke VPC

Hub
(Transit VPC)

CSR-1000v, vMX, SD-WAN & 3rd party
Used for transit services & inter-cloud connections (IPSec)

Inter-Cloud and Hybrid-Cloud VPN

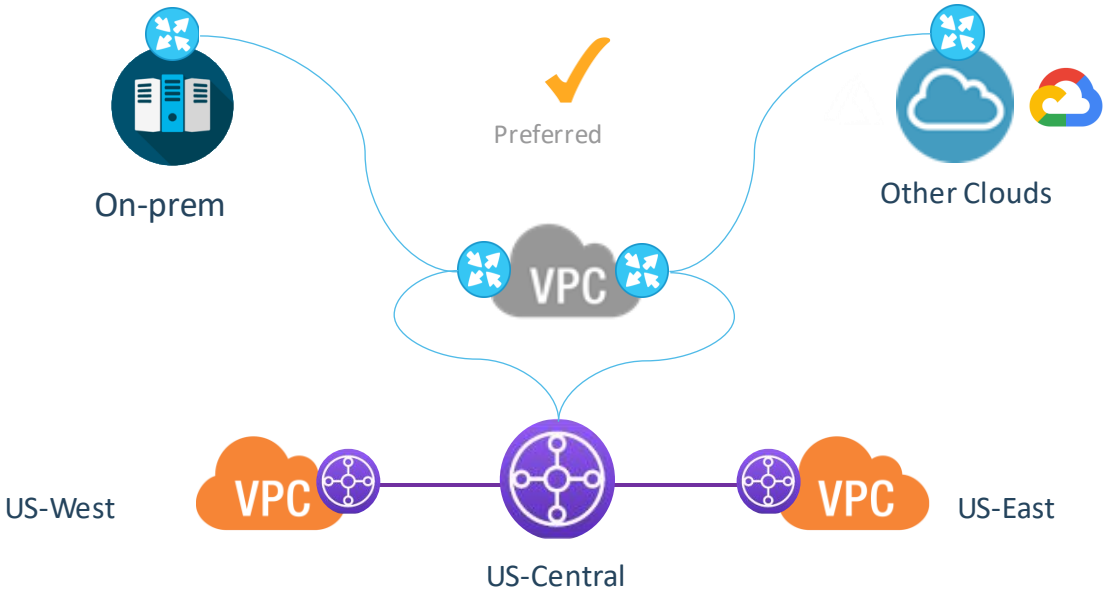
Cloud Provider
Services

aws

Quint@s Quinze

Cloud Networking: AWS

Hub & Spoke – TGW peering + CSR1Kv for Inter-Cloud connectivity



TGW peering architecture
with CSR-1000v

Inter VPC, Inter Region & Inter Cloud
connectivity options

50Gbps per attachment | TGW is a native AWS service

CSR-1000v, vMX, SD-WAN & 3rd party
Used for transit services & inter-cloud connections (IPSec)

Transit Gateway (TGW)
Interconnect hub service for VPC-to-VPC & on-prem (IPSec)

Cloud Provider
Services

aws

Quint@s Quinze

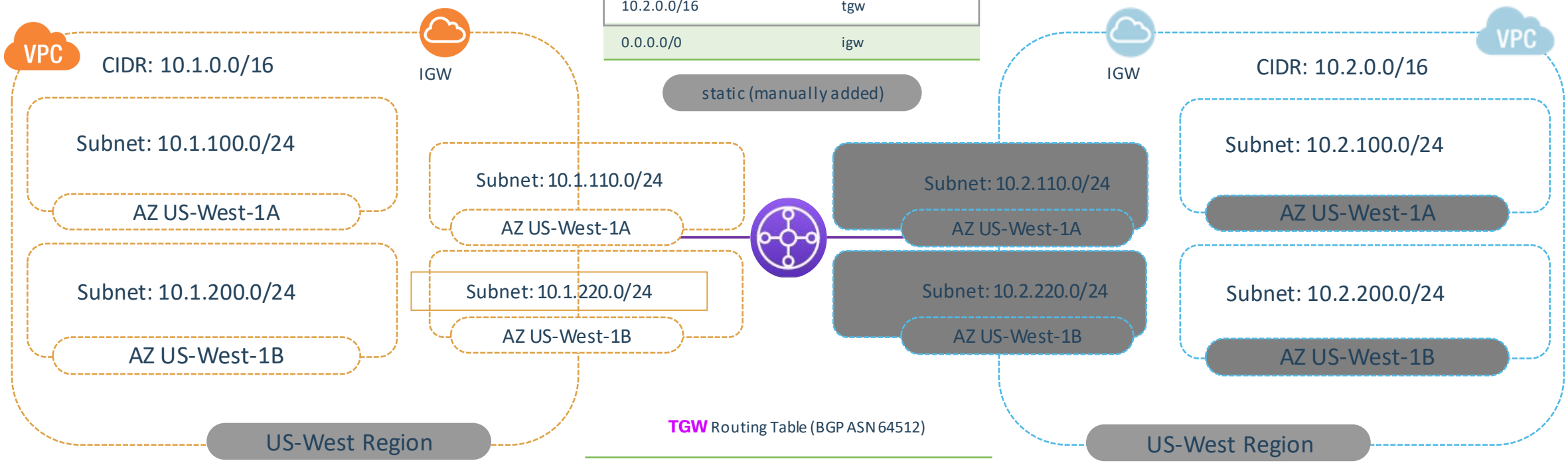
Cloud Networking: AWS

Transit Gateway (TGW)
Interconnect hub service for VPC-to-VPC & on-prem (IPSec)

VPC Routing Table

Destination	Target
10.1.0.0/16	local
10.2.0.0/16	tgw
0.0.0.0/0	igw

static (manually added)



TGW Routing Table (BGP ASN 64512)

Destination	Target
10.1.0.0/16	tgw-attach-vpc1
10.2.0.0/16	tgw-attach-vpc2

* This scenario assumes the same AWS account. When using different accounts, Resource Access Manag
configuration is needed to share the same TGW between them

Quint@s Quinze

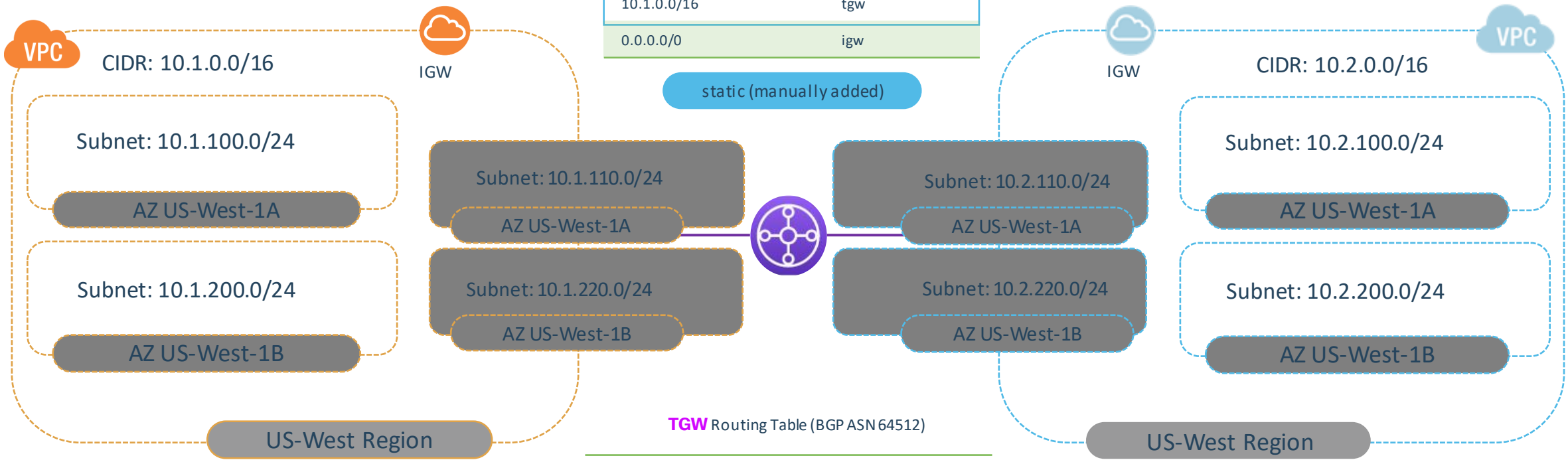
Cloud Networking: AWS

Transit Gateway (TGW)
Interconnect hub service for VPC-to-VPC & on-prem (IPSec)

VPC Routing Table

Destination	Target
10.2.0.0/16	local
10.1.0.0/16	tgw
0.0.0.0/0	igw

static (manually added)



TGW Routing Table (BGP ASN 64512)

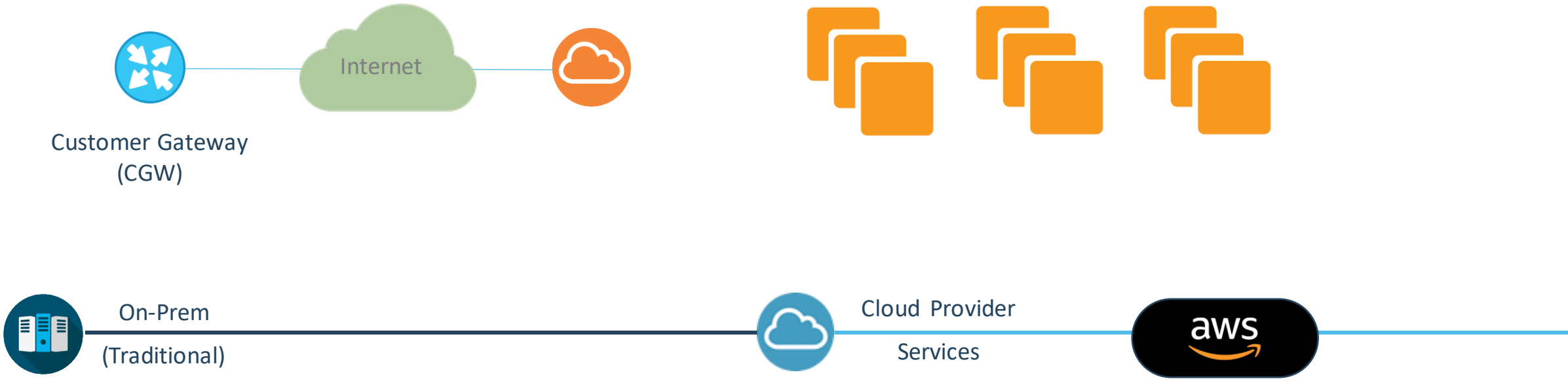
Destination	Target
10.1.0.0/16	tgw-attach-vpc1
10.2.0.0/16	tgw-attach-vpc2

* This scenario assumes the same AWS account. When using different accounts, Resource Access Manag
configuration is needed to share the same TGW between them

Quint@s Quinze

Cloud Networking: AWS

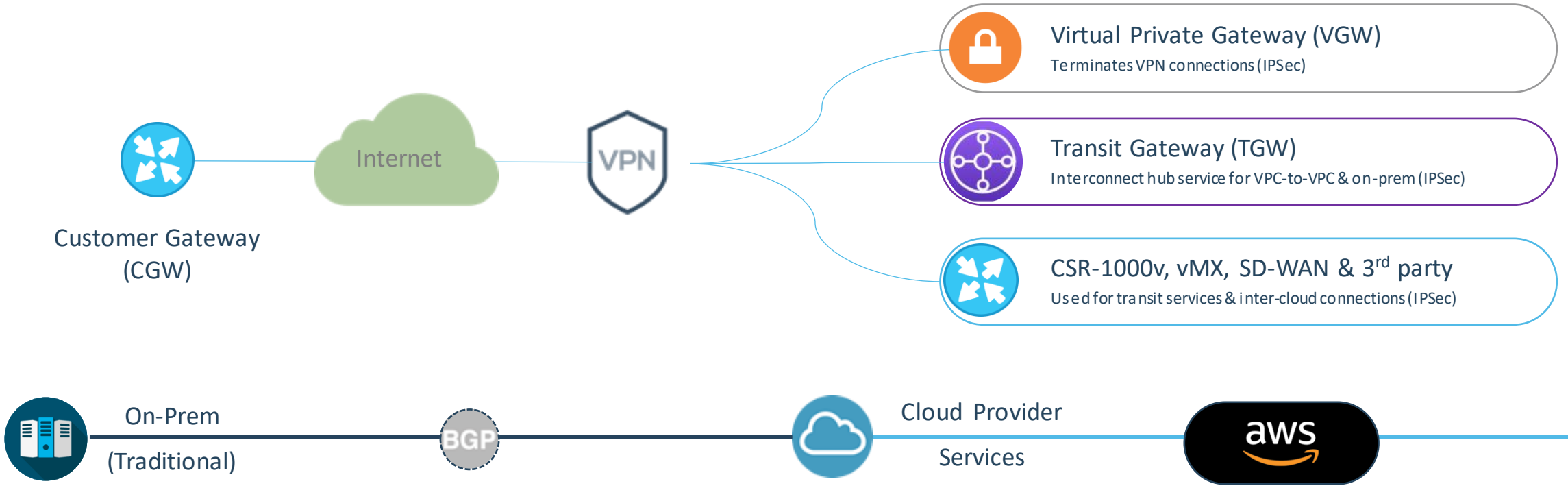
Hybrid-Cloud Connectivity



Quint@s Quinze

Cloud Networking: AWS

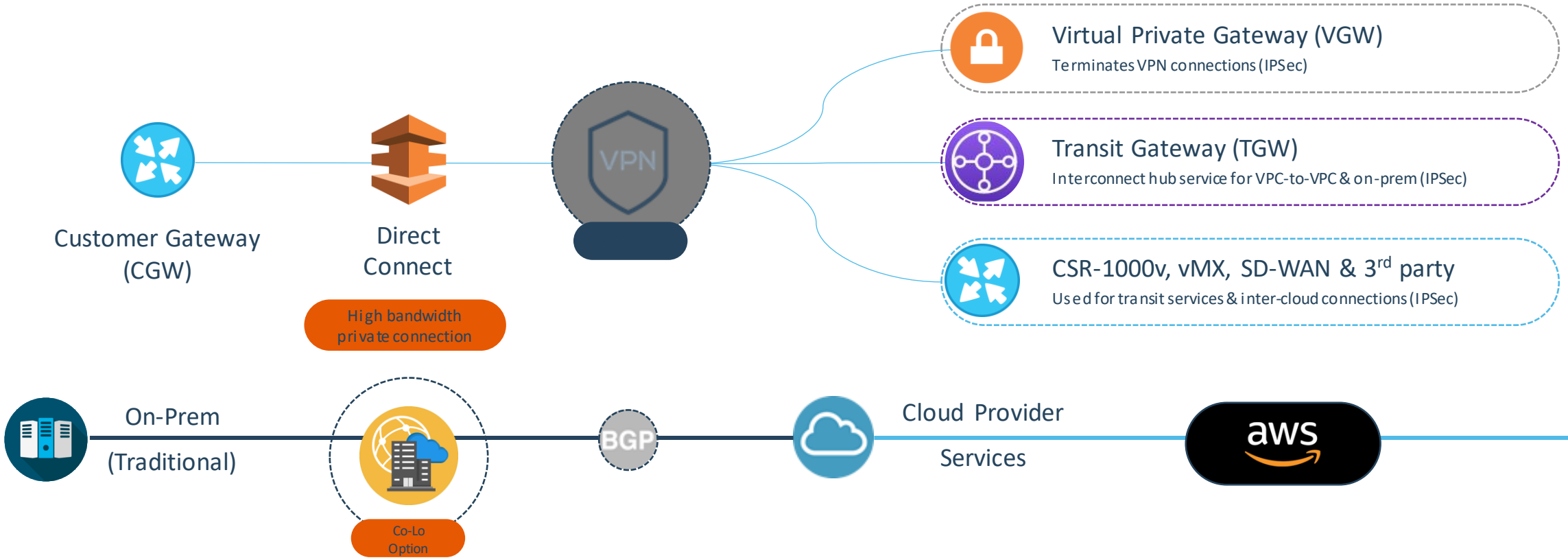
Hybrid-Cloud Connectivity



Quint@s Quinze

Cloud Networking: AWS

Hybrid-Cloud Connectivity

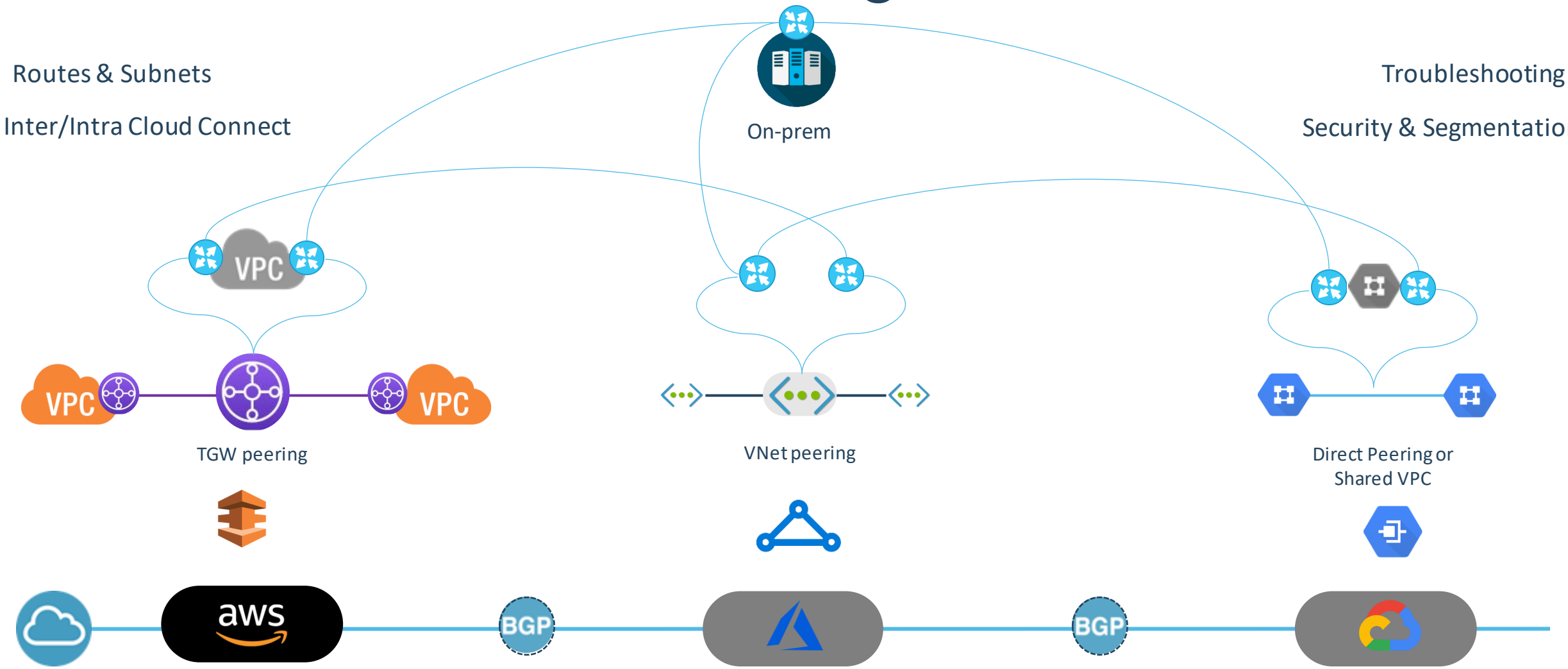


Quint@s Quinze

Multi-Cloud Networking

Routes & Subnets

Inter/Intra Cloud Connect



Troubleshooting

Security & Segmentation

Quint@s Quinze

Conhecendo Cloud ACI

Do básico às nuvens

Quint@s Quinze

ACI: One Network, any location

* Google Cloud in Roadmap

Quint@s Quinze

ACI **Anywhere**

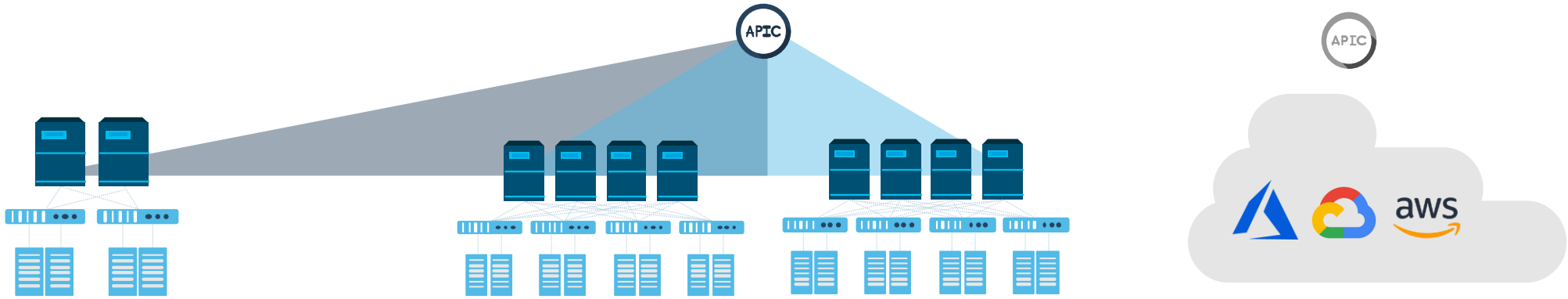
Edge / Remote

Core Data Centers

Public Cloud

IP WAN

IP WAN



Remote Leaf

Multi-Pod

Cloud ACI

Consolidate and normalize network operations **Anywhere!**

*Google Cloud 2021

Quint@s Quinze

The network-admin challenge

Provisioning and monitoring complexity = Risk

NX-OS	ACI	aws		
Separate Infrastructure + VXLAN	Tenant	Account	Subscription/ Resource Group	Account/Project
Data Center	Site/Pod	Region	Region	Region
VRF	VRF	VPC	VNet	VPC
VLAN	Bridge Domain/ Subnet	CIDR/Subnet	Subnet	Subnet
VLAN Tag	EPG	Security Groups	Application/Network Security Groups	Firewall
Access-list (ACL)	Contracts & Filters	Security Group Rules	Security Rules	Firewall Rules

Cloud ACI: Accelerate cloud adoption

In-Cloud networking services automation

Same provisioning model

Same operational model

All cloud-native services available

ACI

Automated

Interconnect, routes, VXLAN/BGP, VPC, TGW, VNet, CSR1K, L4-L7 & more

Configure once

Deploy anywhere (regions, AZs, VPCs, and clouds*) consistently

Secure

Policy normalization, monitoring and encryption

*Multi-Cloud configuration requires Nexus Dashboard Orchestrator

Quint@s Quinze

What are the differences between running ACI on-prem and in the cloud?

On-prem ACI

Cloud ACI

Server Cluster = ACI Site

Runs on 1,3 or more physical servers/VMs

Automated Connectivity

Consistent Operations

Cloud APIC = ACI Site

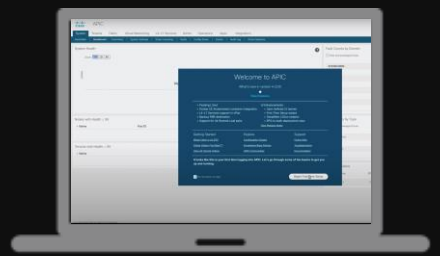
Runs in a Cloud Region as VM/Instance

Starting Setup Utility

Set password, VTEP pool, etc

Covered in Module 1: Episode 2

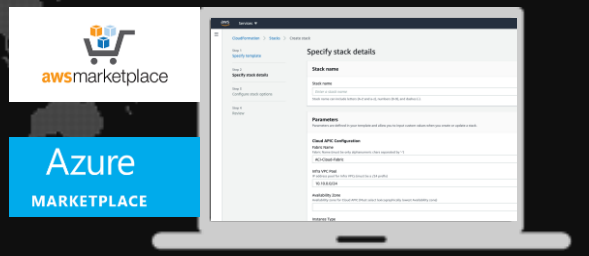
Setup Wizard



Set DNS, NTP, BGP AS, etc

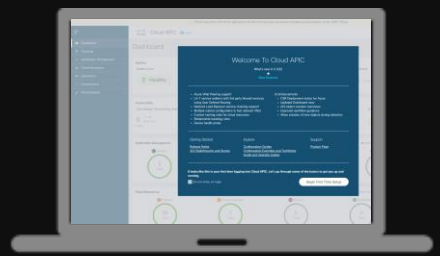
Covered in Module 1: Episode 5

Cloud APIC deployment settings



Set password, Infra pool, Key Pair to use (SSH), etc

Setup Wizard



Set DNS, NTP, BGP AS, regions to manage, etc

Quint@s Quinze

On-prem ACI

Cloud ACI

APIC APIC APIC

Automated Connectivity

Consistent Operations

Nexus 9000 Spines

Nexus 9000 Leaves

Virtual ACI
(vPod)

APIC

vTap

No Cisco hardware or hypervisor needed

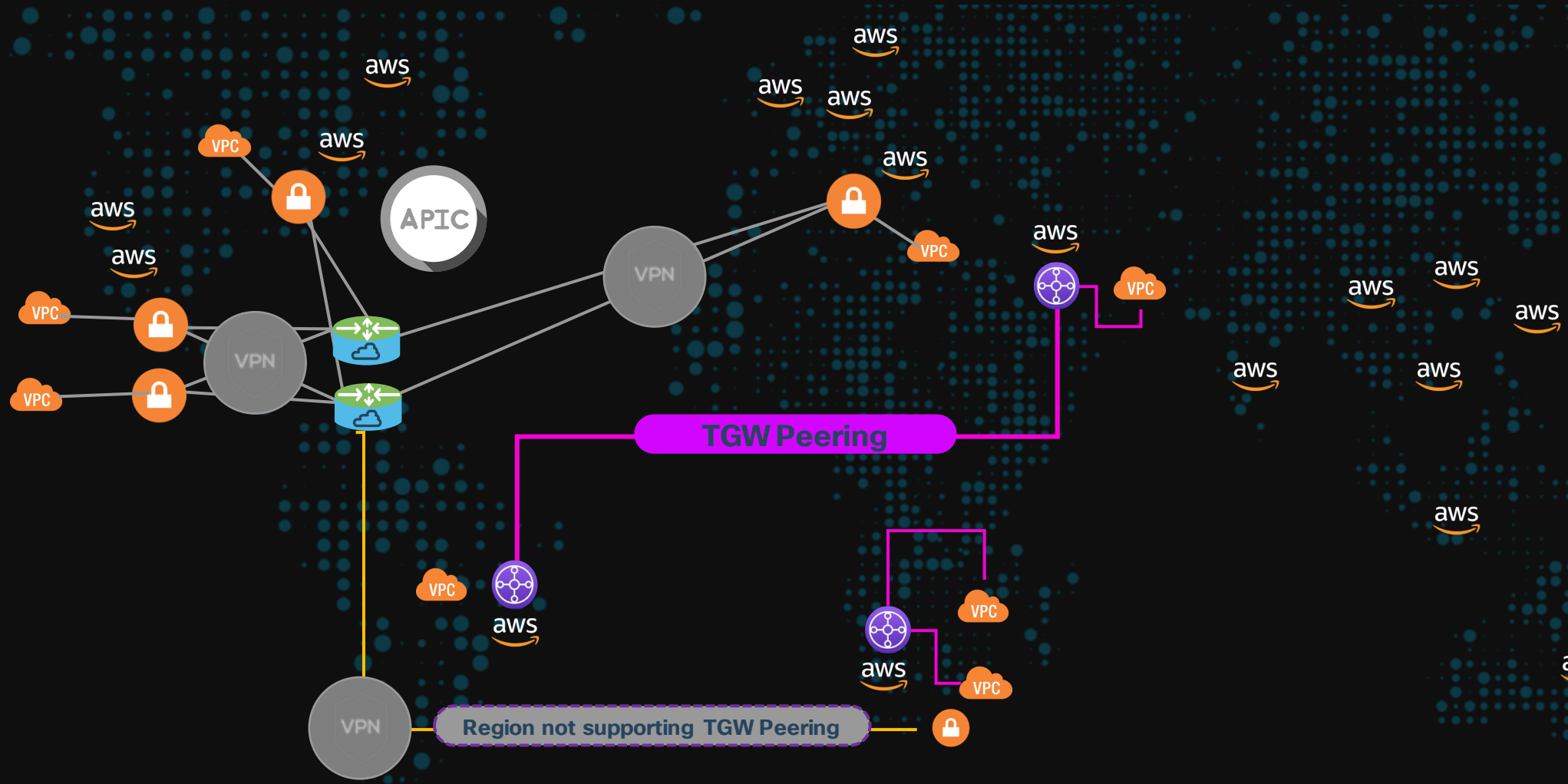
Runs on Cloud Infrastructure natively

Automates and Secures Cloud Connectivity
Instance/VMs and Services across VPCs/VNets, & Regions

Quint@s Quinze

How is connectivity automated and secured without Spine or Leaf Nodes?

Single APIC can manage multiple AWS regions



Cloud ACI

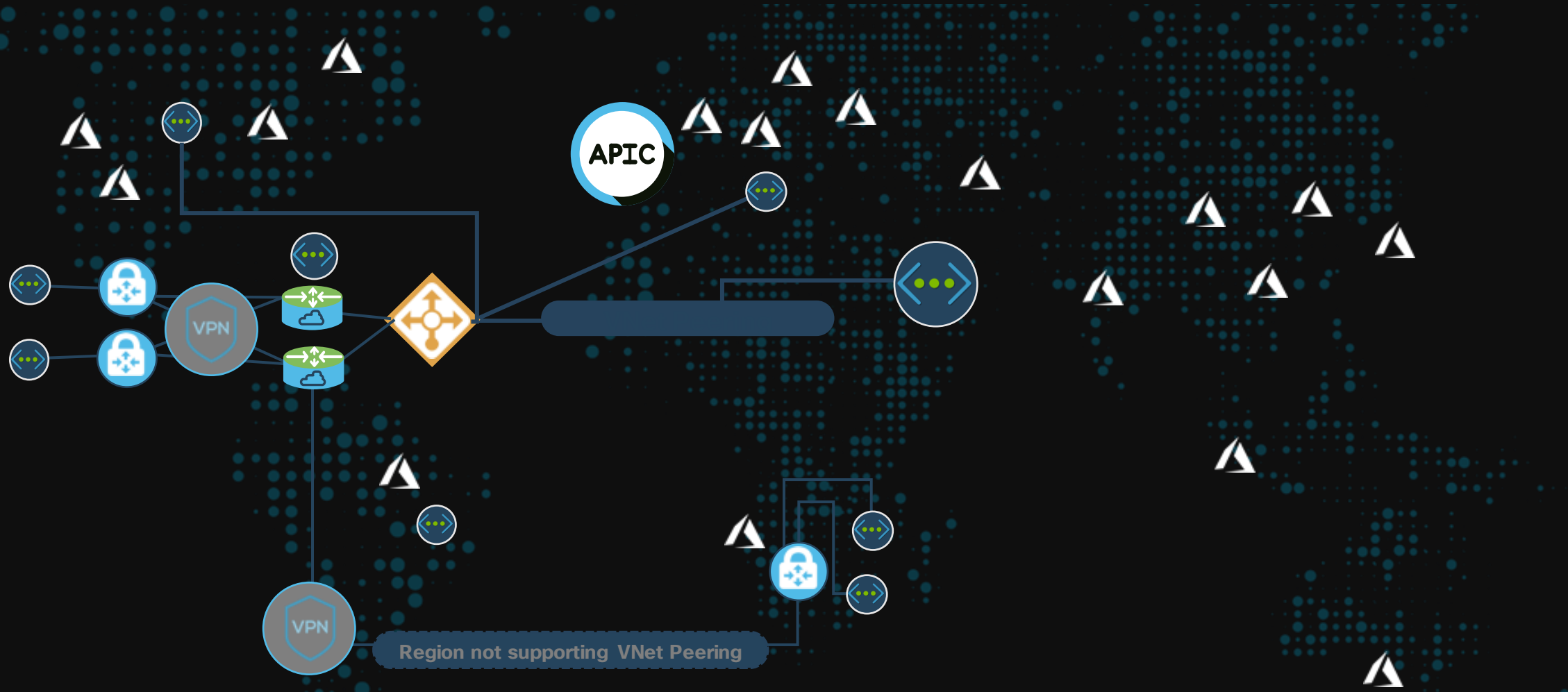
Automated TGW, VGW, CSR, Routes and VPN deployment

aws

*Other topologies a[illegible]

Quint@s Quinze

Single APIC can manage multiple Azure regions



Cloud ACI

Automated VNet Peering, VNG, CSR, NLB, UDR and VPN deployment

*Other topologies a[illegible]e

Quint@s Quinze

How is the logical network configuration different in Cloud **ACI**?

On-prem **ACI**

Cloud **ACI**

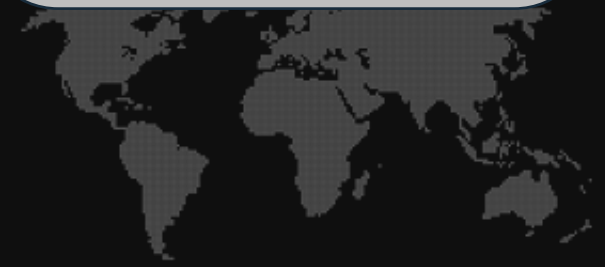
APIC APIC APIC

APIC aws

APIC Azure

Automated Connectivity

Consistent Operations



Default Tenants

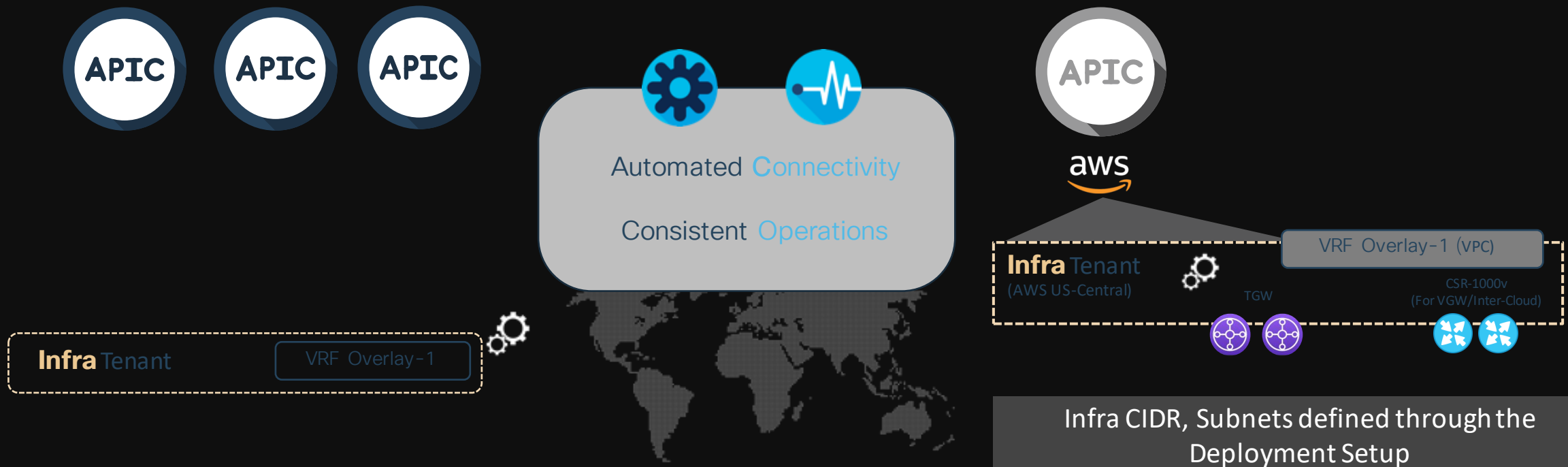
Infra Tenant — VRF Overlay-1

Common Tenant — VRF default

Management Tenant — VRF oob

On-prem ACI

Cloud ACI



Infra CIDR, Subnets defined through the Deployment Setup

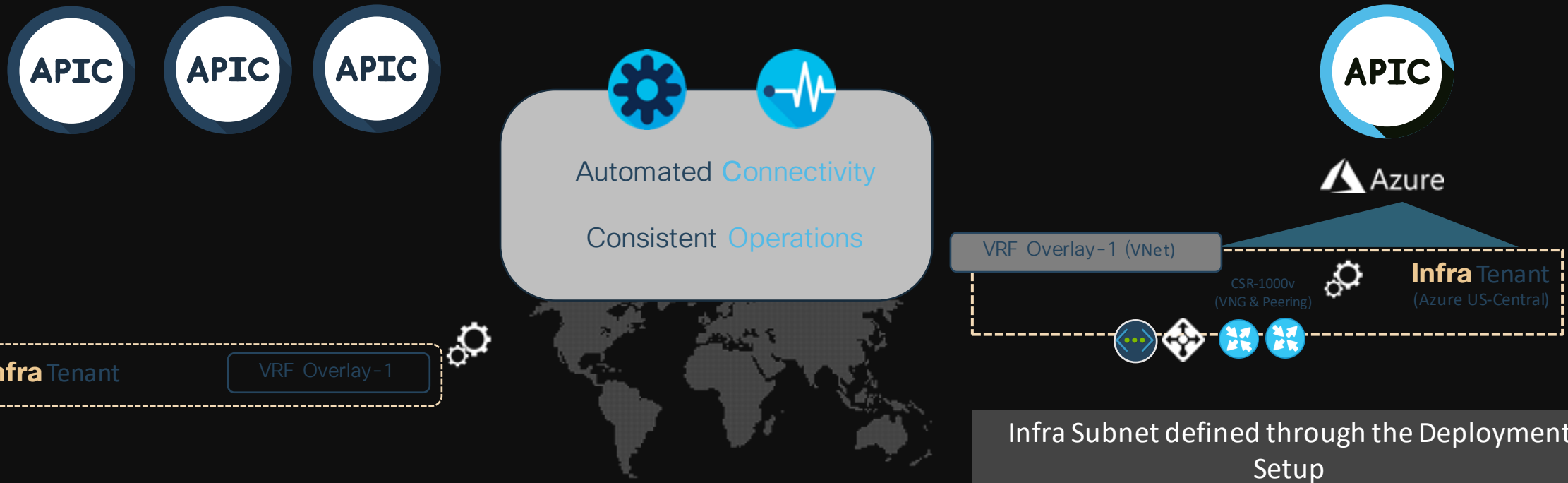
Regions to manage, deployment type and BGP AS defined during Initial setup

Common tenant is also available to be used

Quint@s Quinze

On-prem ACI

Cloud ACI



Infra Subnet defined through the Deployment Setup

Regions to manage, deployment type and BGP AS defined during Initial setup

Common tenant is also available to be used

Quint@s Quinze

Logical Network

5 Steps

1. Create Tenant, VRF
2. Create Application Profile
3. Create EPGs
4. Create Contracts
5. Create External (L3 Out) EPG

On-prem ACI

Cloud ACI

APIC APIC APIC

APIC APIC

aws Azure

Automated Connectivity

Consistent Operations

Infra Tenant

Workload Tenant A

Workload Tenant B

Infra Tenant — AWS Account — Azure Resource Group

Workload Tenant A — AWS Account — Azure Resource Group

Workload Tenant B — AWS Account — Azure Resource Group

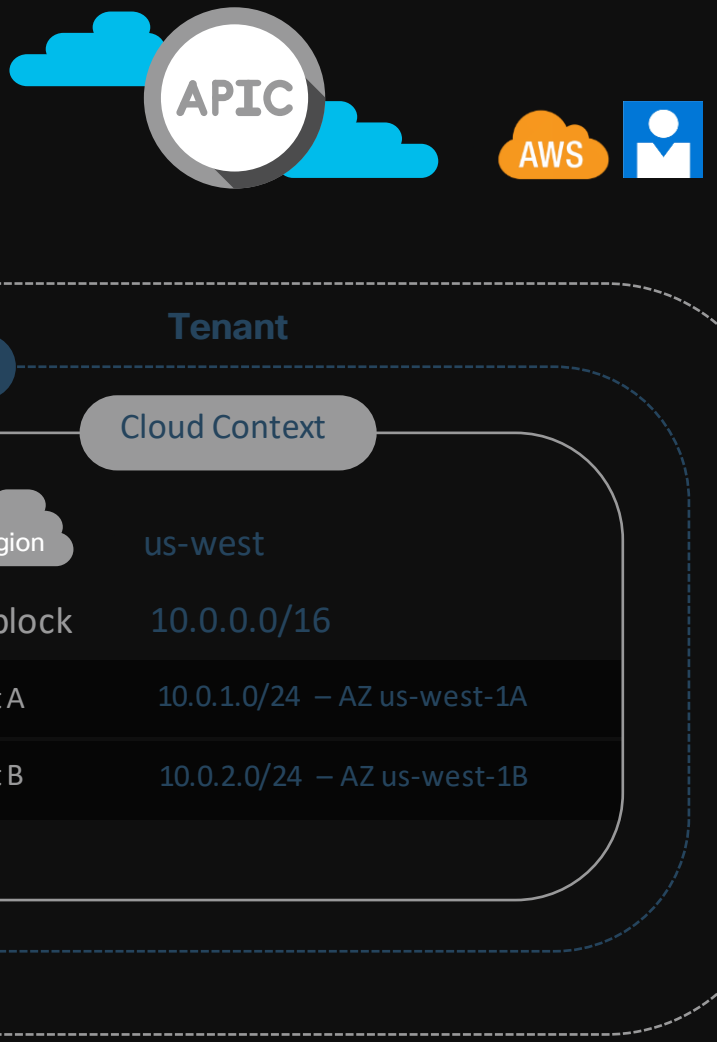
Cloud APIC automatically configures the Workload Tenant network

For that to work, the right privileges need to be set in the tenant account/RG

Logical Network

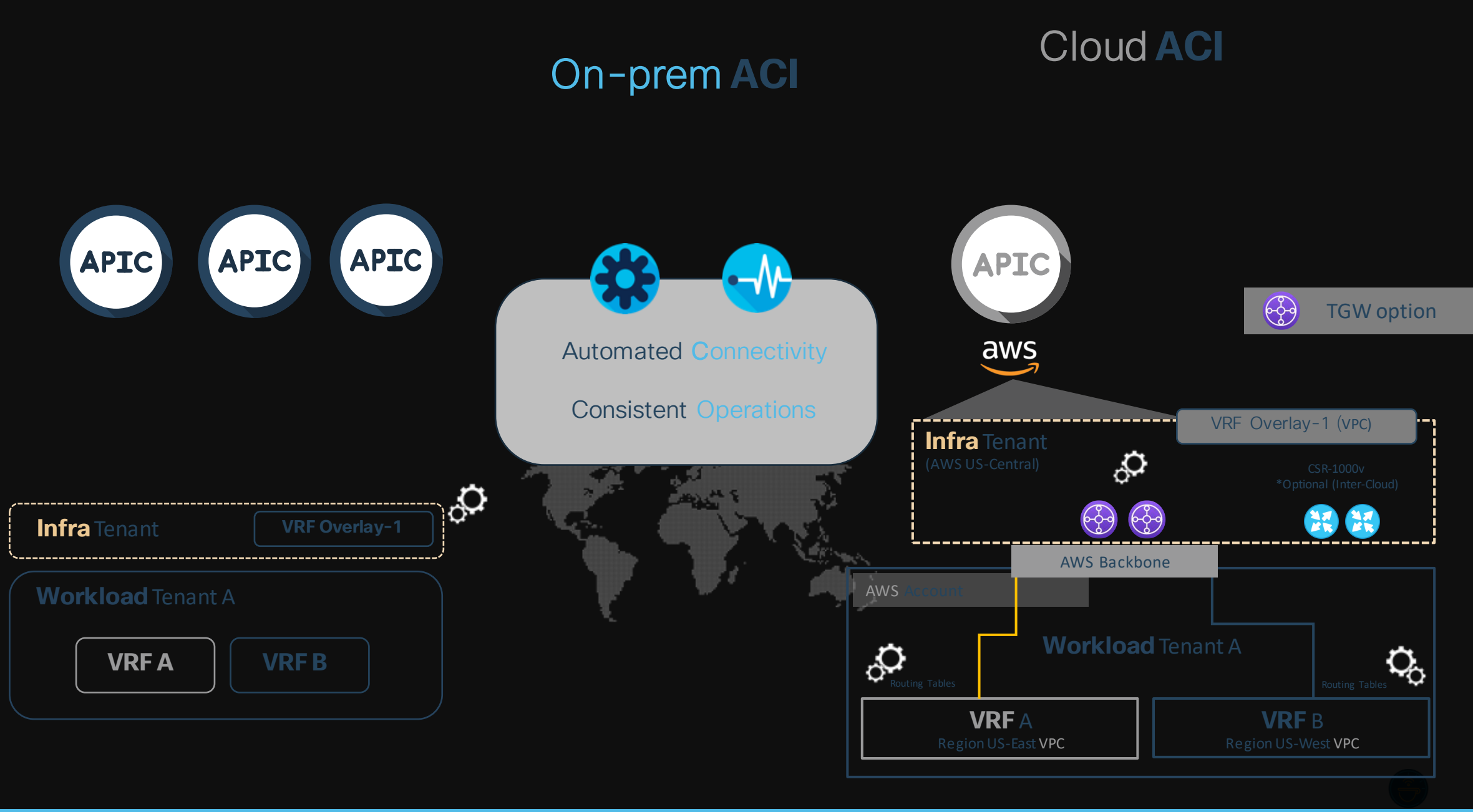
5 Steps

1. Create Tenant, VRF and Cloud Context
2. Create Application Profile
3. Create EPGs
4. Create Contracts
5. Create External (L3 Out) EPG



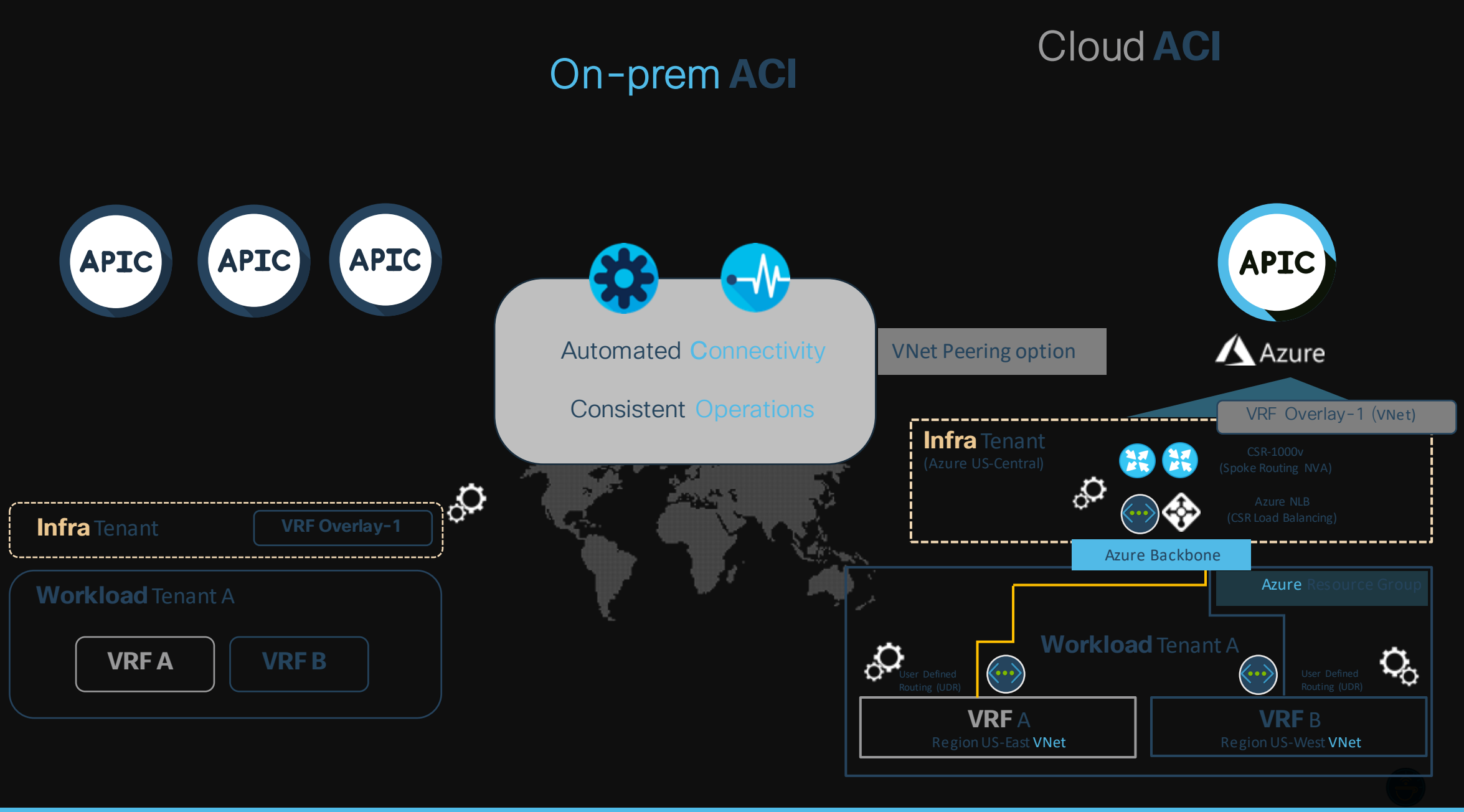
On-prem ACI

Cloud ACI

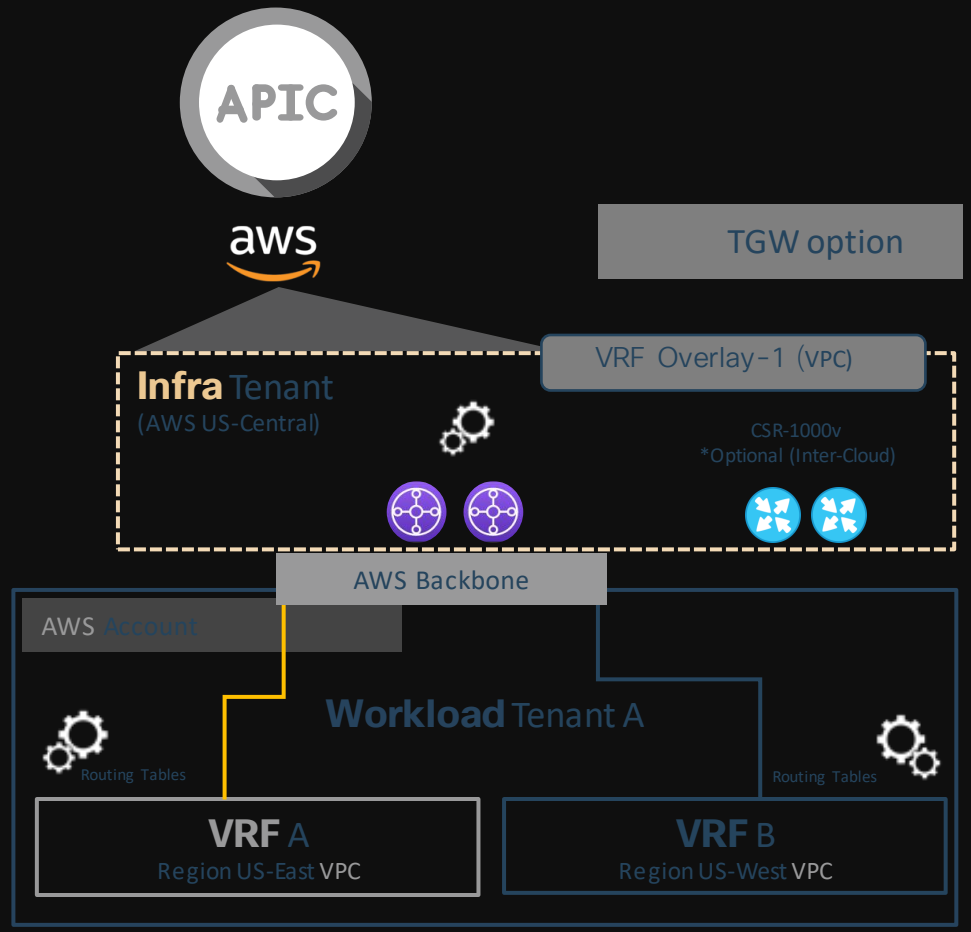

On-prem ACI
Cloud ACI
APIC
APIC
APIC
Automated Connectivity
Consistent Operations
APIC
aws
TGW option
Infra Tenant
(AWS US-Central)
VRF Overlay-1 (VPC)
CSR-1000v
*Optional (Inter-Cloud)
Infra Tenant
VRF Overlay-1
Workload Tenant A
VRF A
VRF B
AWS Backbone
AWS Account
Workload Tenant A
Routing Tables
Routing Tables
VRF A
Region US-East VPC
VRF B
Region US-West VPC

On-prem ACI

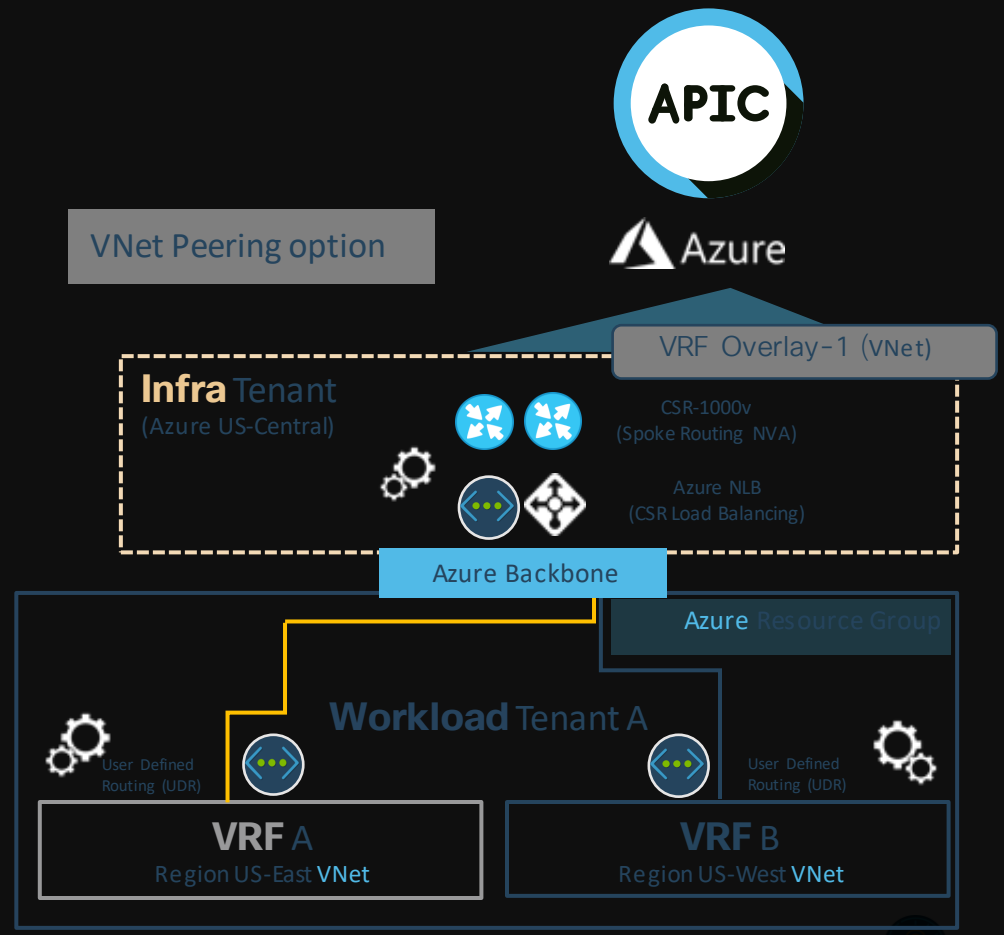
Cloud ACI


On-prem ACI
Cloud ACI
APIC
APIC
APIC
Automated Connectivity
Consistent Operations
VNet Peering option
APIC
Azure
VRF Overlay-1 (VNet)
Infra Tenant
(Azure US-Central)
CSR-1000v
(Spoke Routing NVA)
Azure NLB
(CSR Load Balancing)
Azure Backbone
Infra Tenant
VRF Overlay-1
Workload Tenant A
VRF A
VRF B
Azure Resource Group
Workload Tenant A
User Defined Routing (UDR)
User Defined Routing (UDR)
VRF A
Region US-East VNet
VRF B
Region US-West VNet

Cloud ACI



Cloud ACI



Logical Network

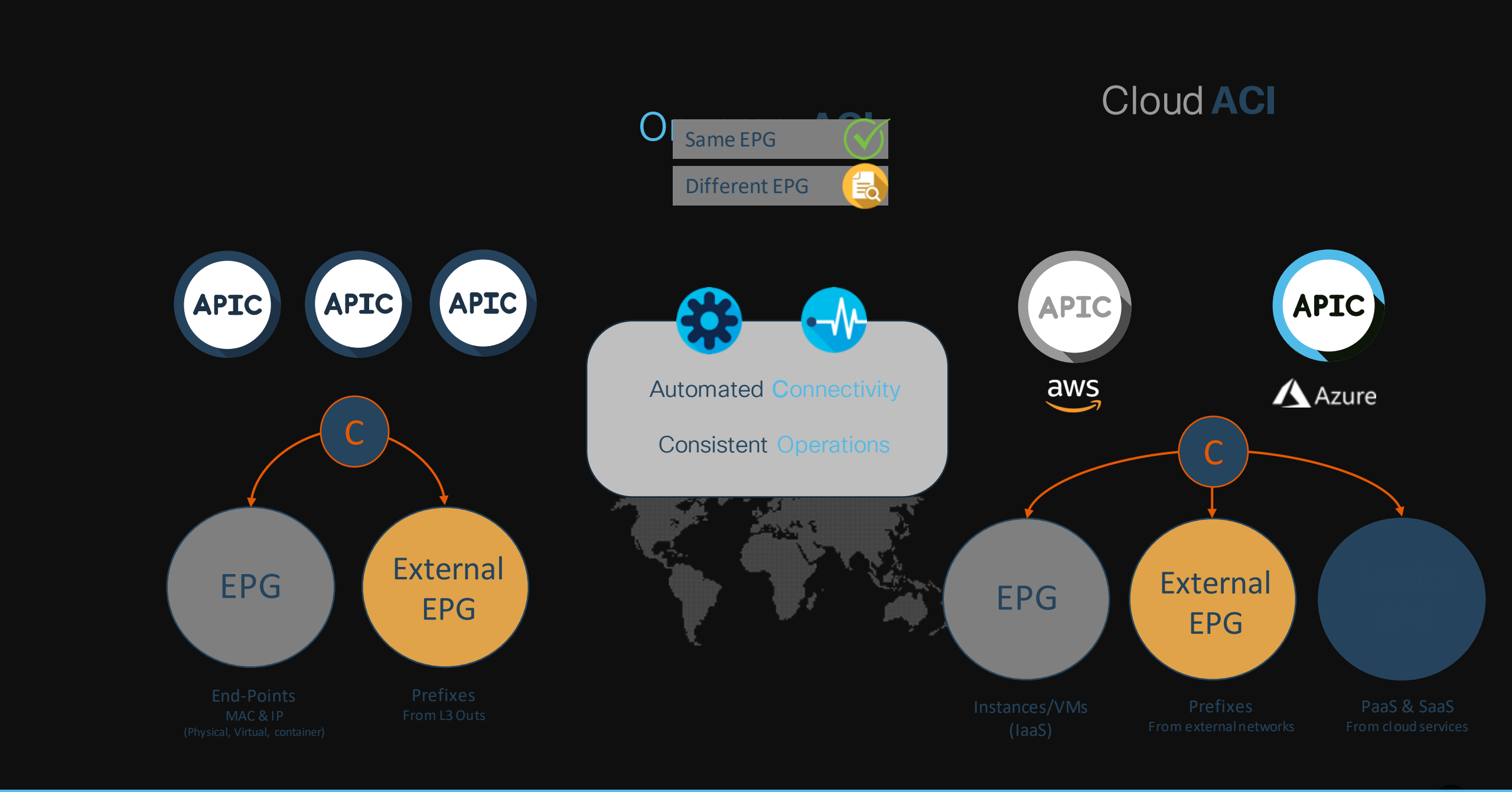
5 Steps

1. Create Tenant, VRF and Cloud Context
2. Create Application Profile
3. Create EPGs
4. Create Contracts
5. Create External (L3 Out) EPG

Logical Network

5 Steps

1. Create Tenant, VRF and Cloud Context
2. Create Application Profile
3. Create EPGs
4. Create Contracts
5. Create External (L3 Out) EPG



Quint@s Quinze

Cloud **ACI**

Same EPG

Different EPG

APIC APIC APIC

EPG

APIC aws

APIC Azure

Workload Tenant A **VRF A**

App Profile MyApp

EPG A

Static assignment

µSeg (Attribute-Based Selector)

µSeg (Attribute-Based Selector)

Region, AZ, IP, Custom (Key, Value)

Workload Tenant A **VRF A**

App Profile MyApp

EPG A

No Bridge Domain

EPGs in Cloud APIC are always µSeg through attributes using selectors

On-prem **ACI**

Cloud **ACI**

APIC APIC APIC

External EPG

APIC aws

APIC Azure

Workload Tenant A — VRF A

App Profile MyApp

External EPG (L3 Out)

0.0.0.0/0

Prefix Match Selector

Workload Tenant A — VRF A

App Profile MyApp

Prefix Match Selector

External EPG

0.0.0.0/0

Available on Cloud ACI 5.1(2) and later

Cloud ACI

APIC aws

APIC Azure

Automated Connectivity

Consistent Operations

Workload Tenant A

VRF A

App Profile MyApp

Service EPG

PaaS and SaaS

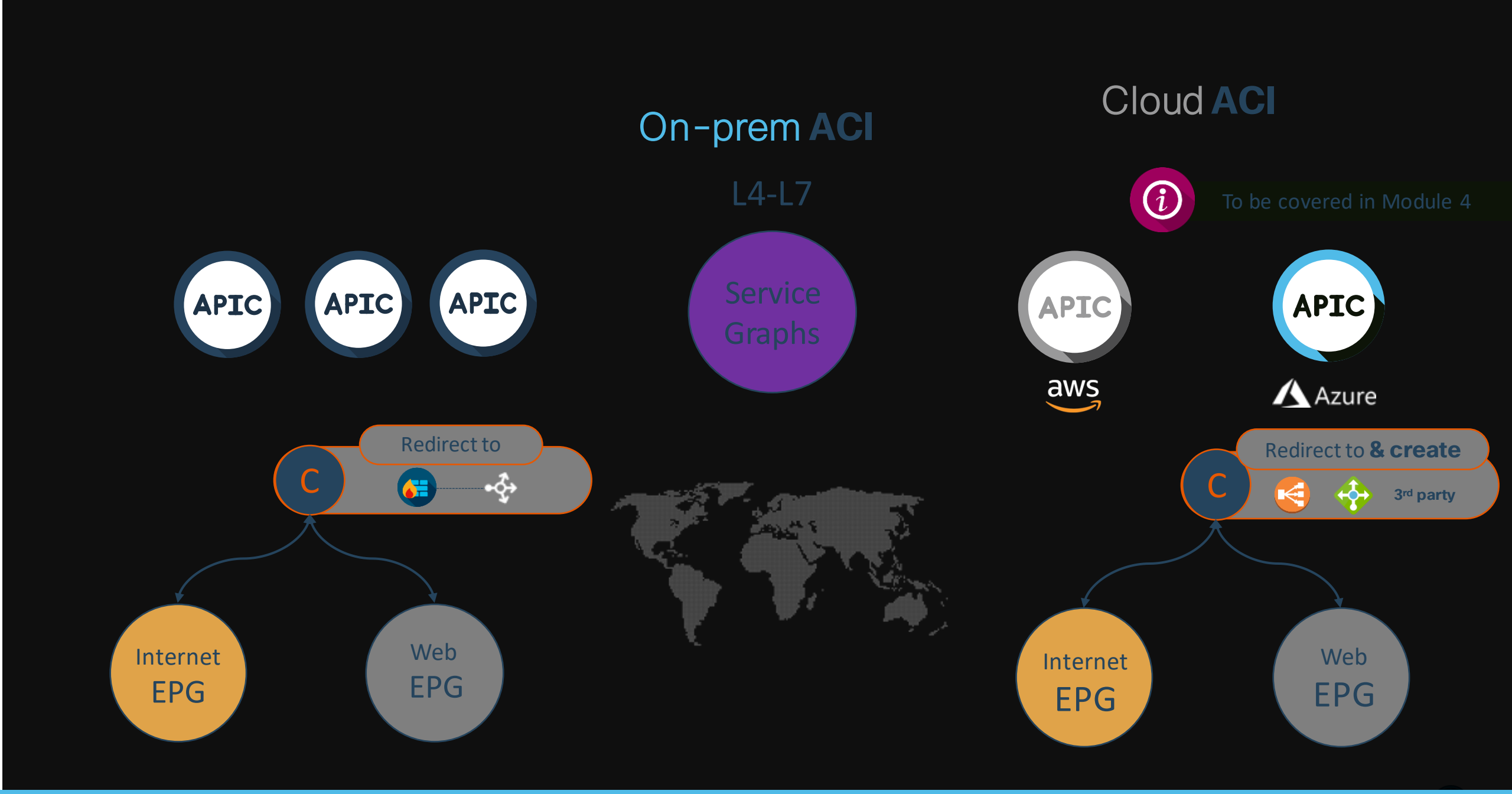
Name, Subnet and other attributes

PaaS and SaaS

Cloud Native

Cloud Native Managed

3rd Party


On-prem ACI
L4-L7
Service Graphs
APIC
APIC
APIC
Redirect to
C
Internet EPG
Web EPG
Cloud ACI
To be covered in Module 4
APIC
aws
APIC
Azure
Redirect to & create
C
3rd party
Internet EPG
Web EPG

Casos de uso

Tudo que pensamos para facilitar o dia-a-dia

Quint@s Quinze

Cloud Challenges

How?

- Lift + Shift
- Re-platform
- Modernize Apps
- DRaaS

Migration

Integration

Learning Curve

What about

Security

Hyper-V aws

Time-to-Value

Maximize Cloud-Native Services

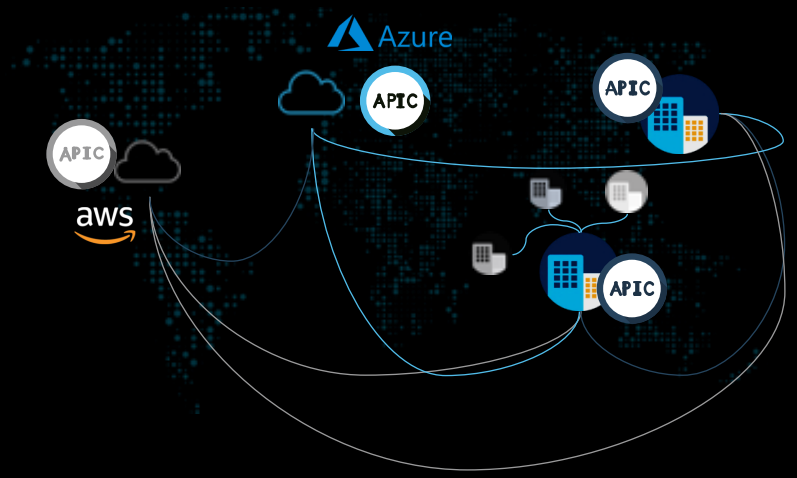
24x7 Operations

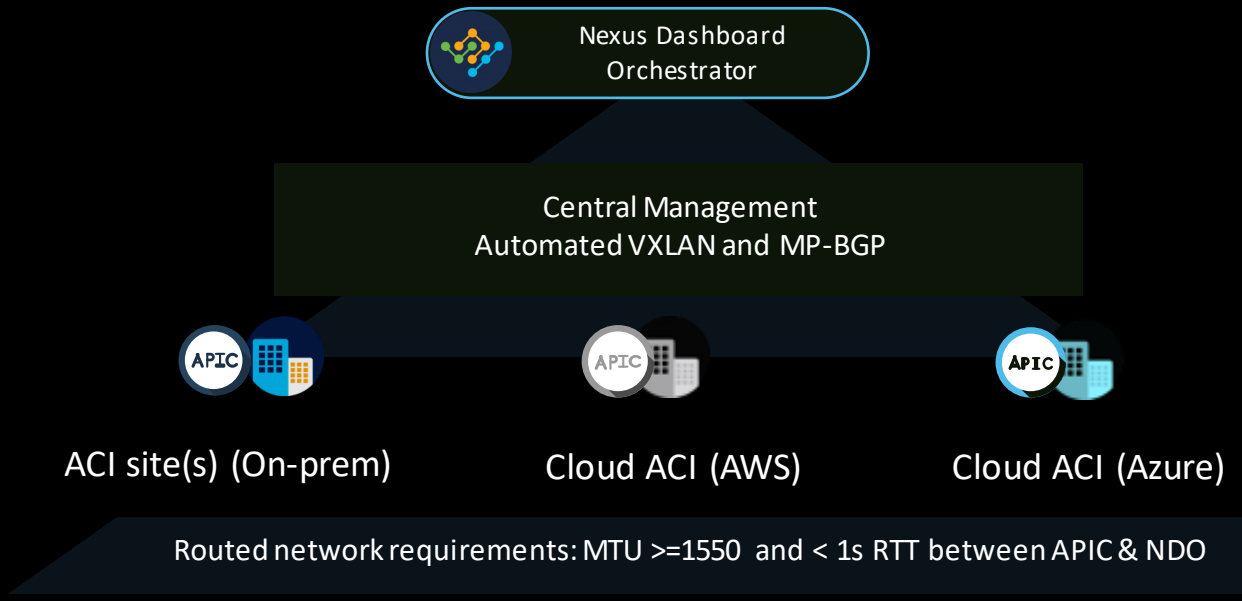
100%

Multi-Site ACI

On-Prem & Cloud

Business continuity/DR/DRaaS | DC/Cloud Interconnect | VM Mobility & Cloud Migration





Automate Cloud and DC Interconnect. Provision **once**, deploy **anywhere**

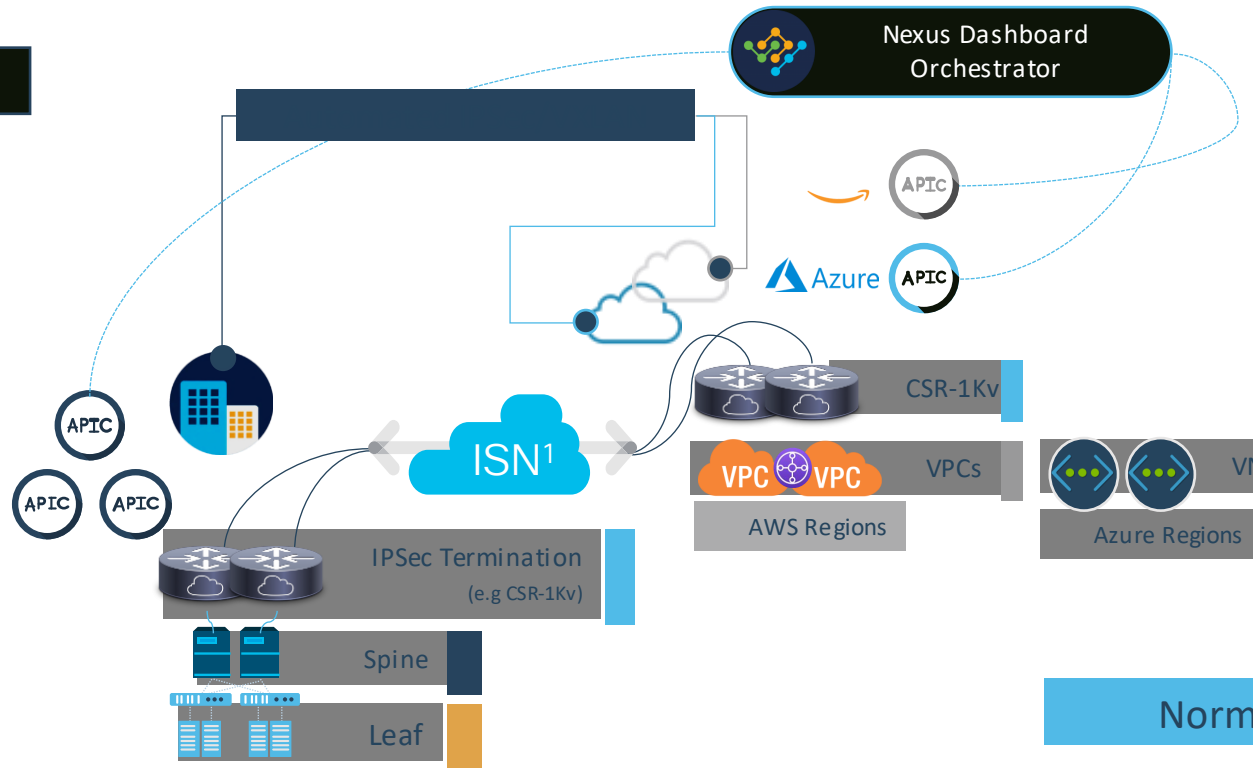
Quint@s Quinze

Multi-Site ACI

Hybrid Cloud

Up to 12 Sites

Reduce learning curve | Cloud Interconnect | Consistent security policy



On-prem requirements and considerations:

Inter-Site Network required[1]

IPSec on-prem termination device(s) are required. IPSec Configuration can be downloaded from NDO

MP-BGP, VXLAN, routes and OSPF configurations are automated by NDO

Common deployments

- DRaaS
- Cloud Migration
- On-Prem-Cloud Integration
- Normalize operations and security policy

Simplify and **accelerate** your journey to the cloud

[1] ISN may traverse the Internet or use a dedicated connection (AWS Direct Connect/Express Route)

*In addition to Jumbo Frames (1550+ MTU) and 1 second RTT from Nexus Dashboard ND[illegible]PIC

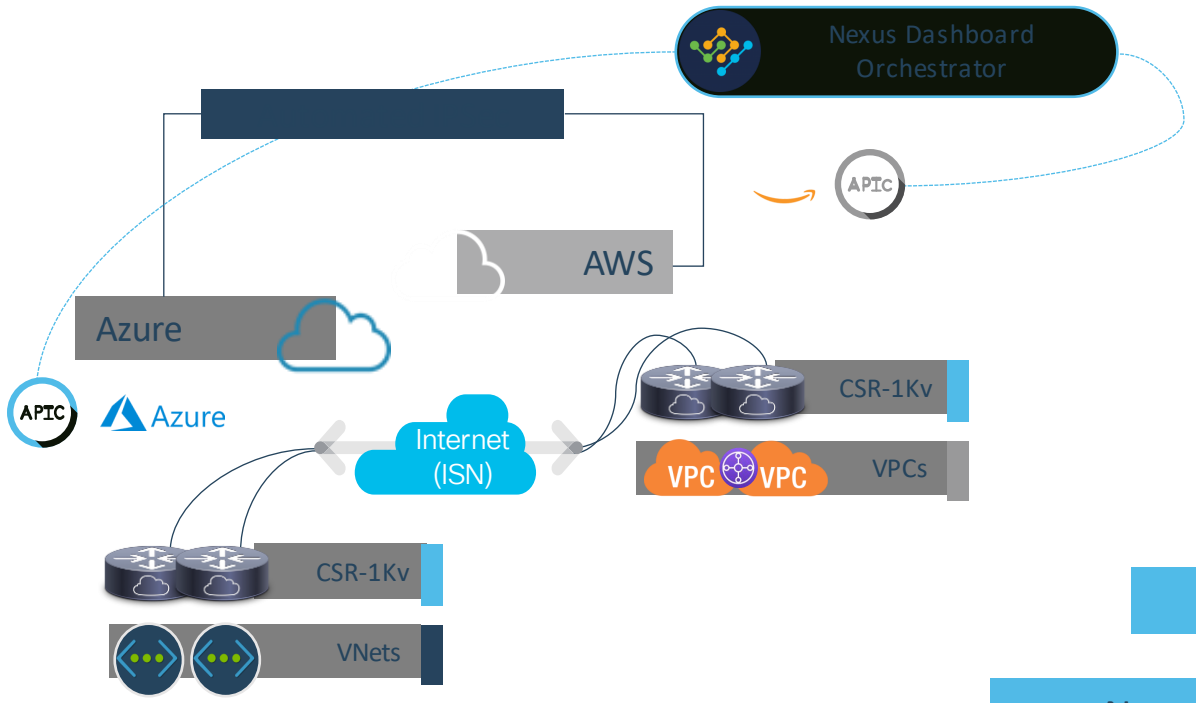
Quint@s Quinze

Multi-Site ACI

Cloud Only

Up to 12 Sites

Reduce learning curve | Cloud Interconnect | Consistent security policy



Cisco **CSR-1000v** is deployed and configured automatically in Cloud ACI

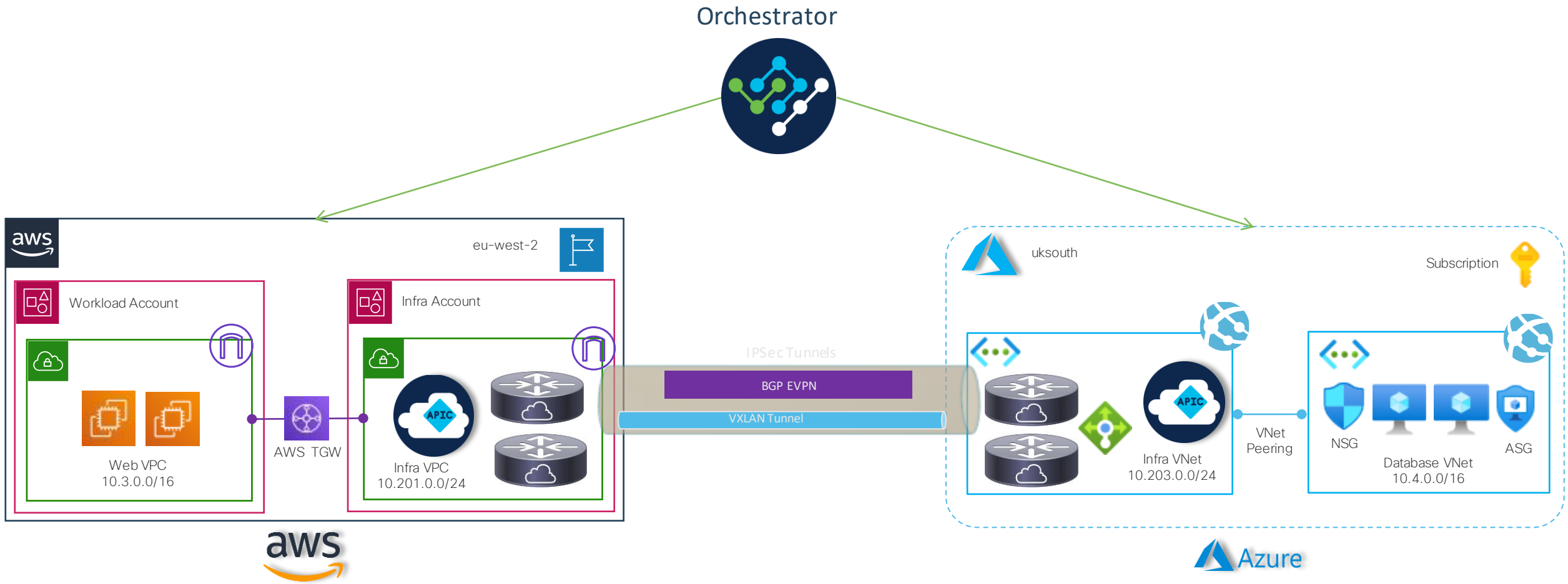
IPSec, MP-BGP, VXLAN, routes and OSPF configurations are **automated** by Nexus Dashboard **NDO**

Common deployments

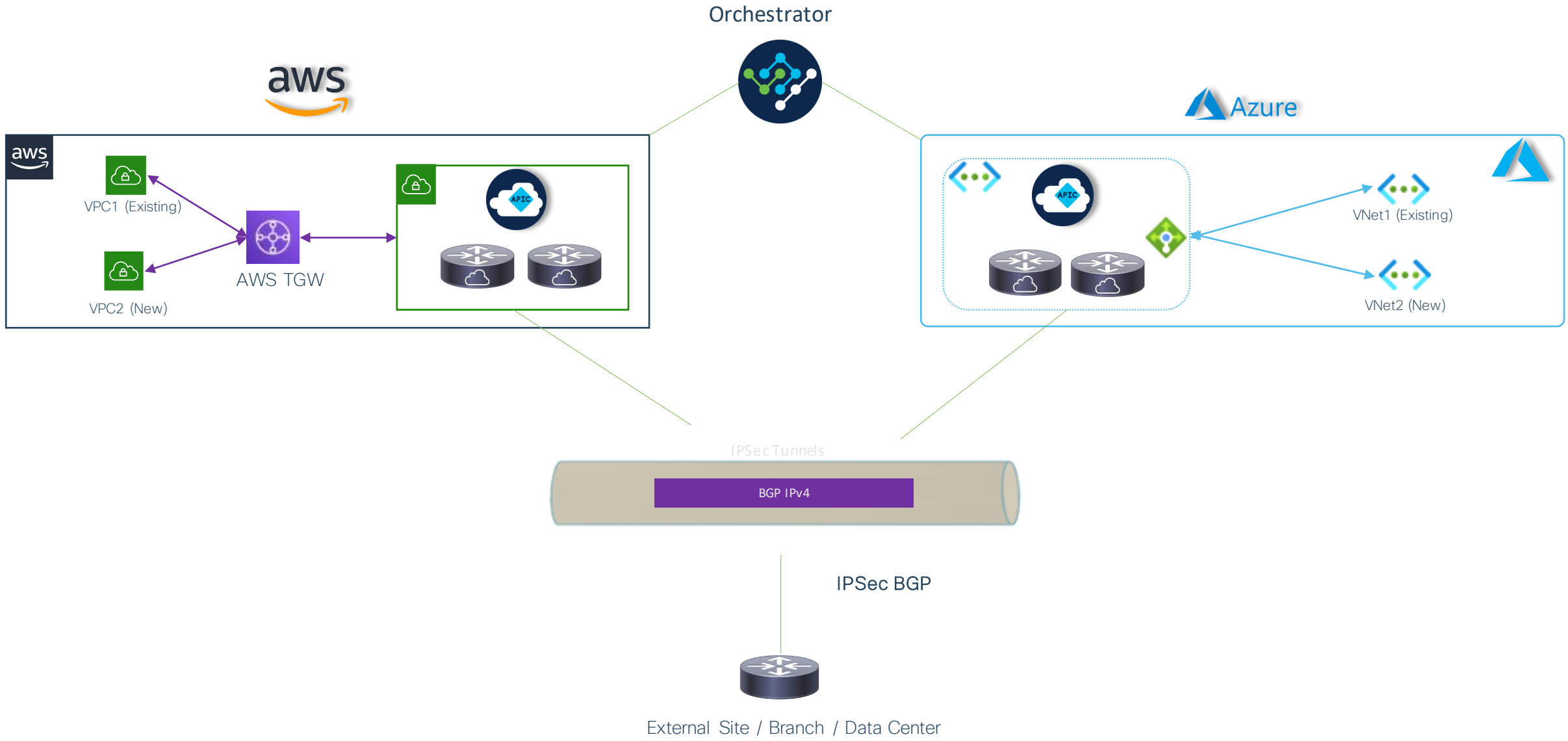
- Multi-Cloud
- Migration and failover
- Phased-change implementations
- Normalize operations and security policy

Simplify, automate and **normalize** Multicloud operations

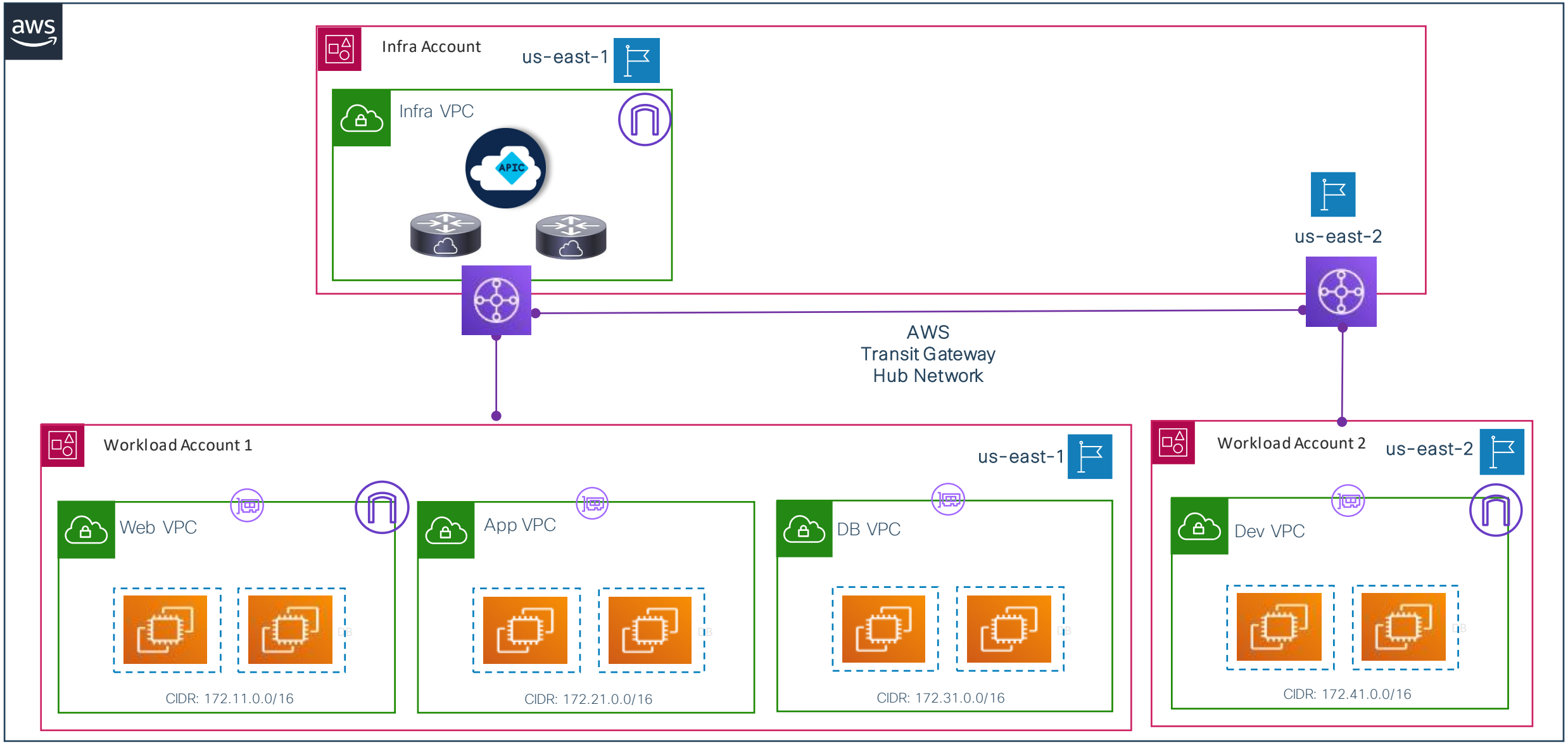
Quint@s Quinze



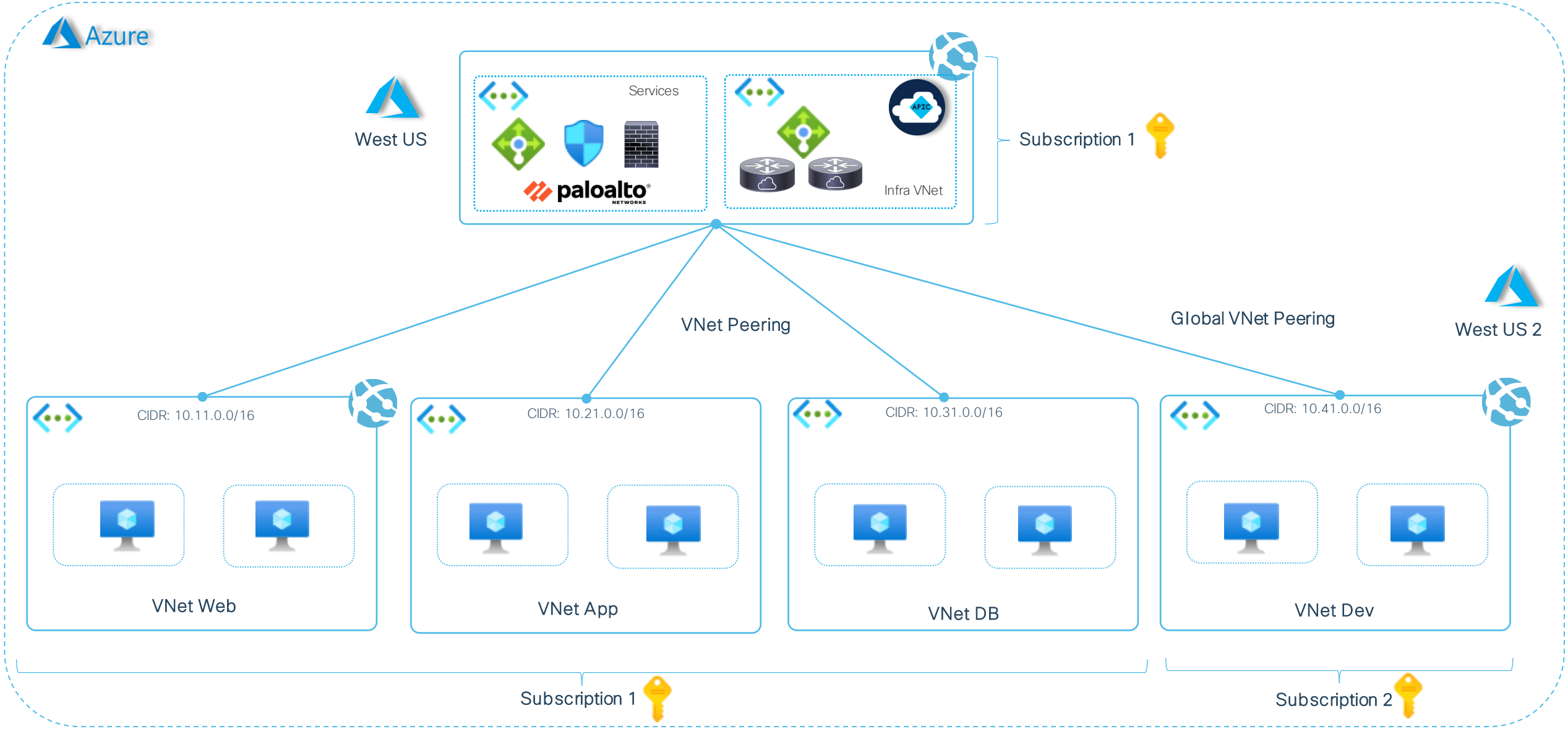
ACI Multi-Cloud between AWS and Azure with BGP EVPN (policy stretch)



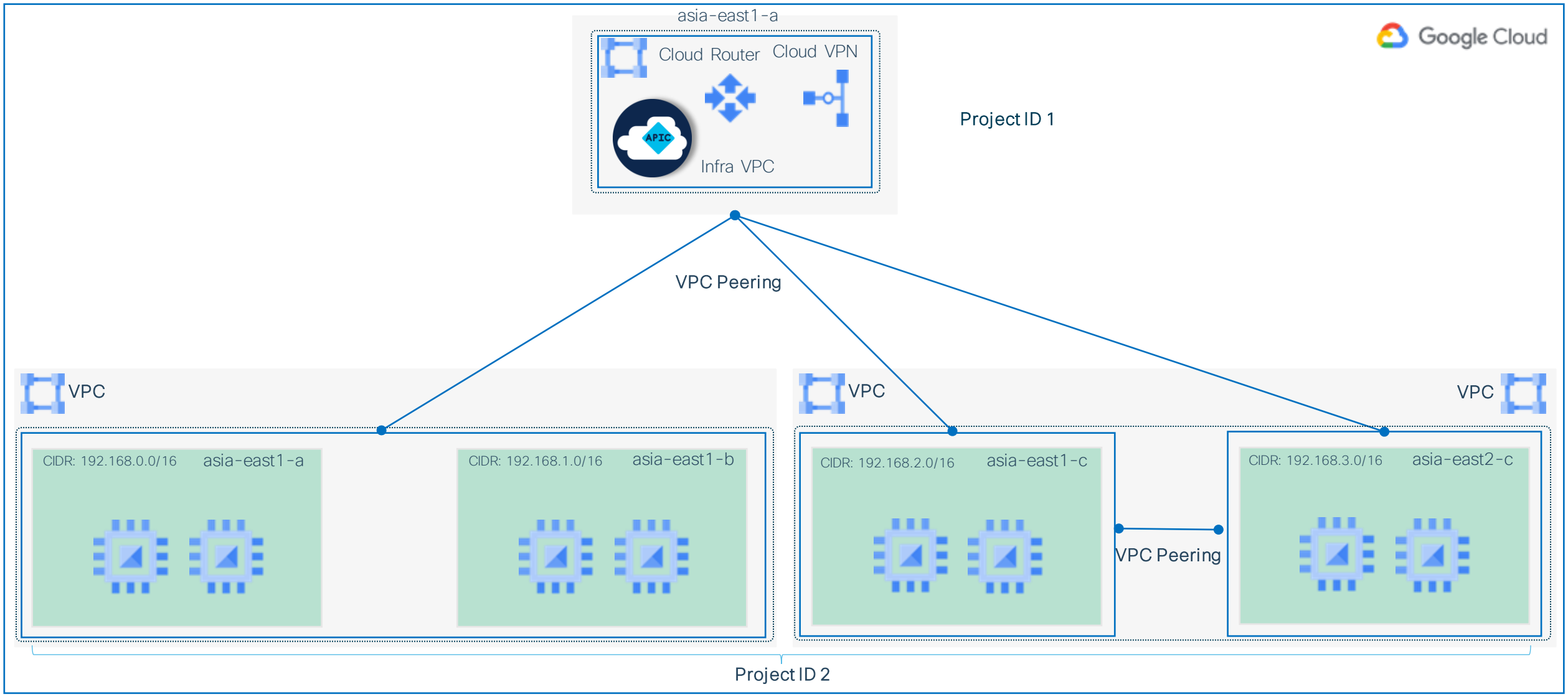
Automating External Connectivity to AWS and Azure with IPSec BGP on Cloud Router or TGW



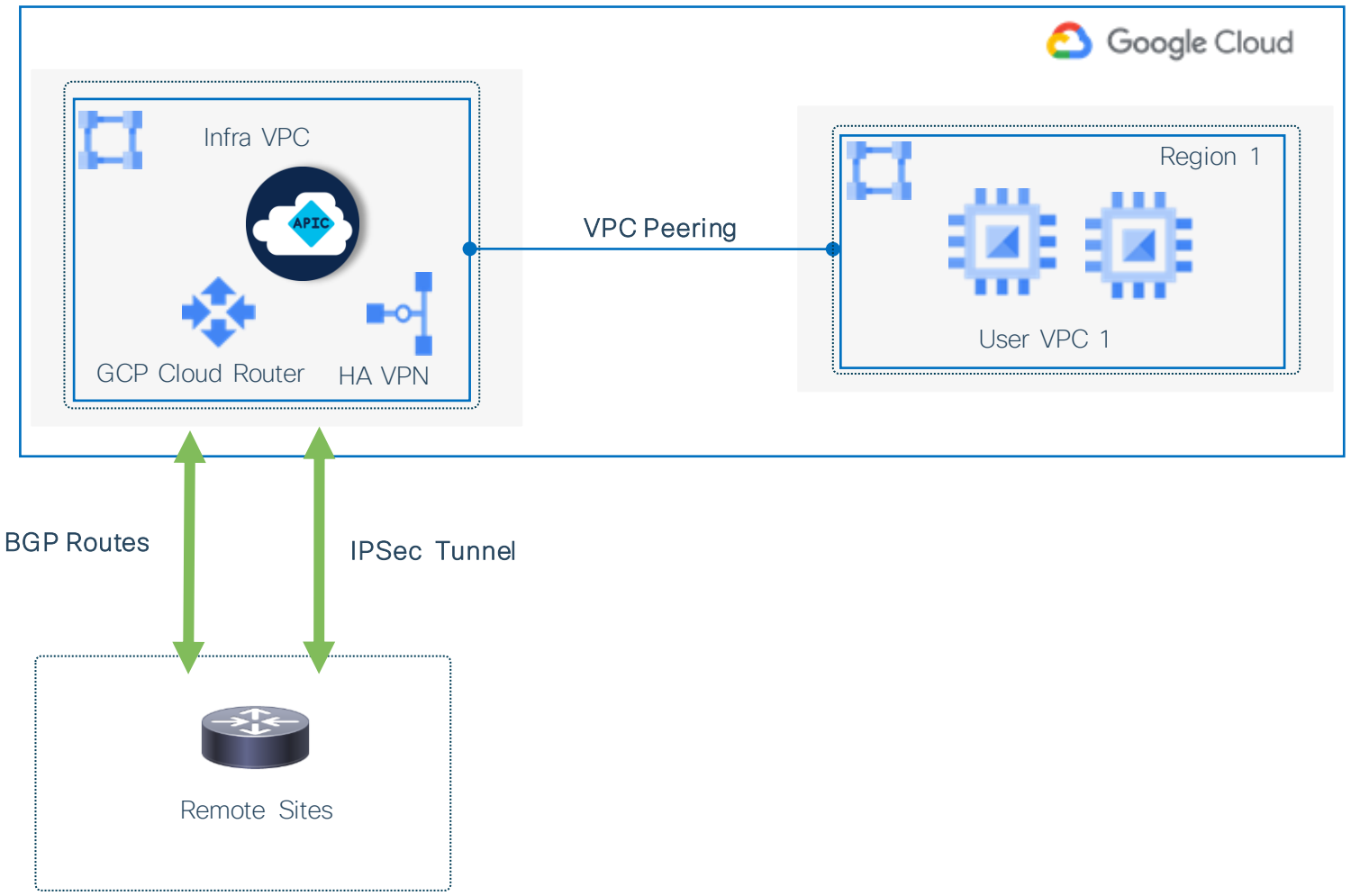
Cloud ACI in AWS



Cloud ACI in Azure

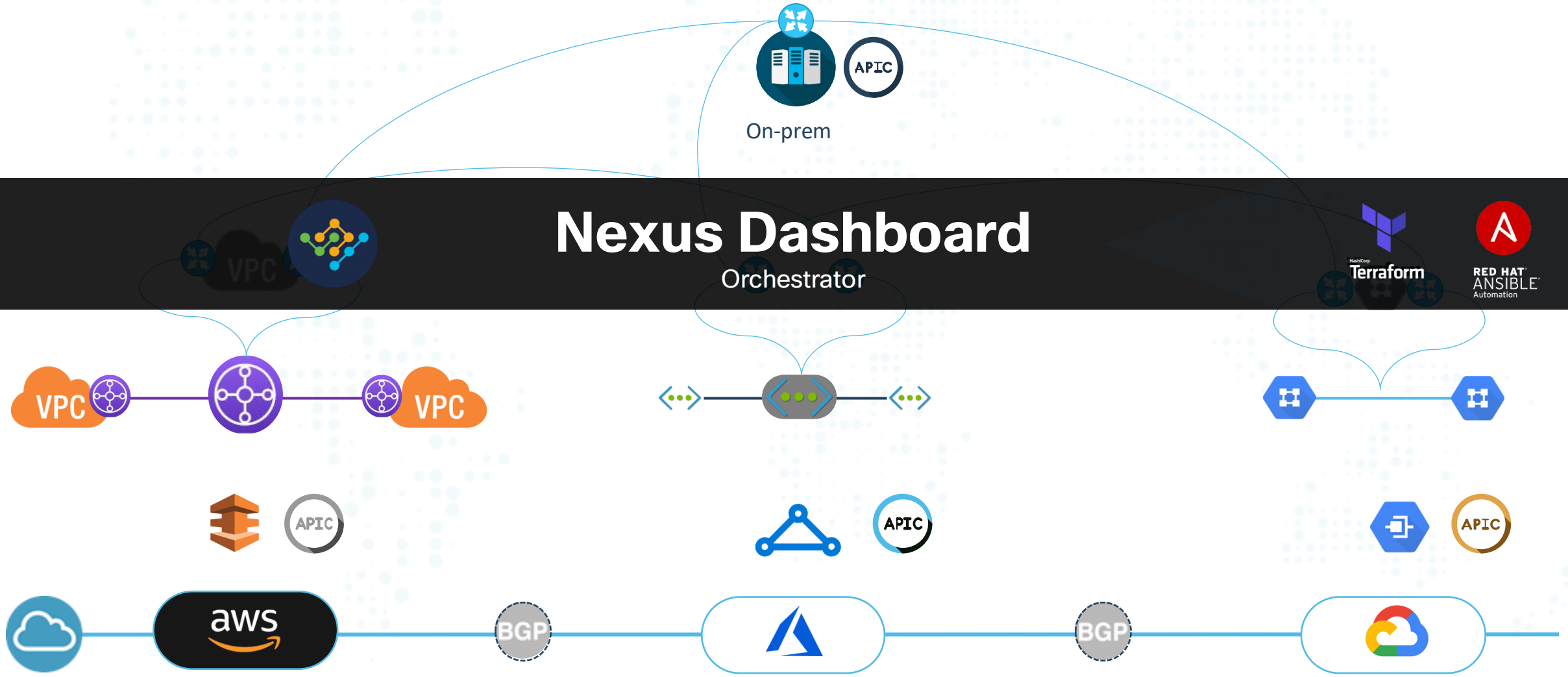


Cloud ACI in GCP

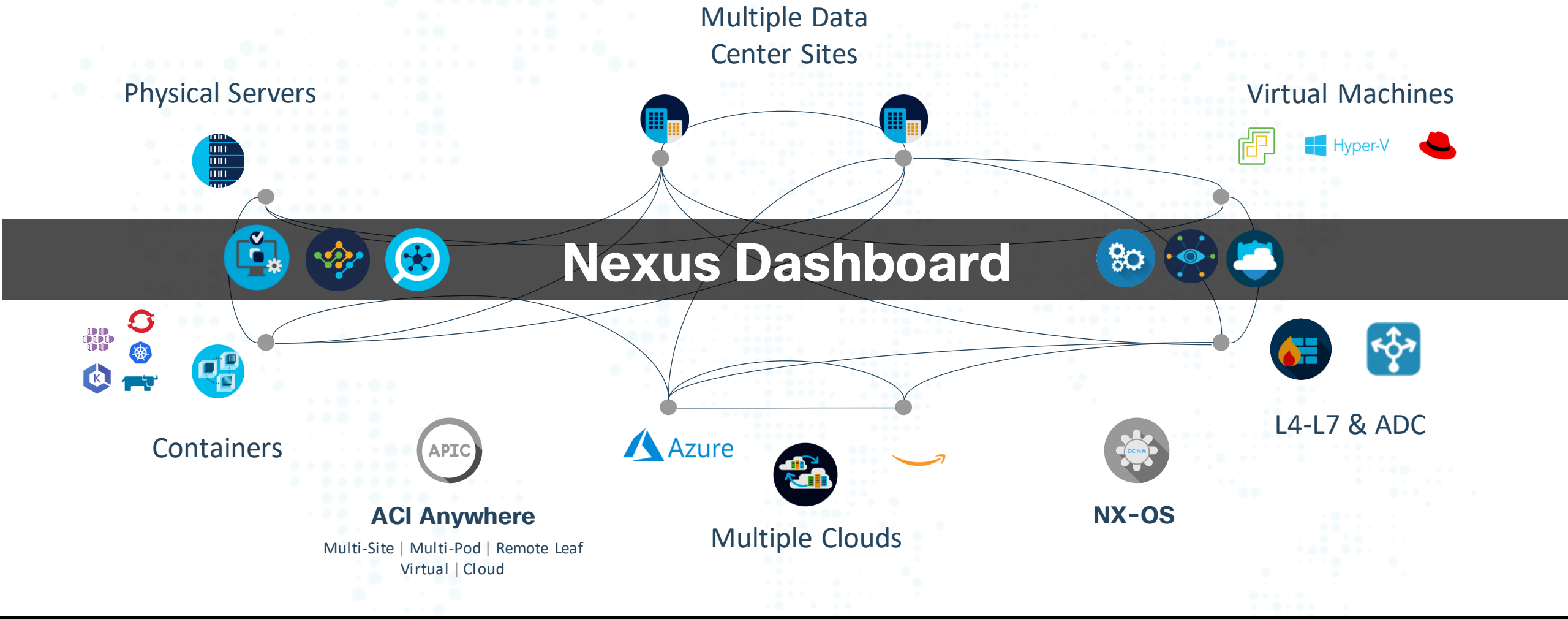


Enabling External Connectivity from GCP to a Remote Site

Automated Multi-Cloud Interconnect



Quint@s Quinze

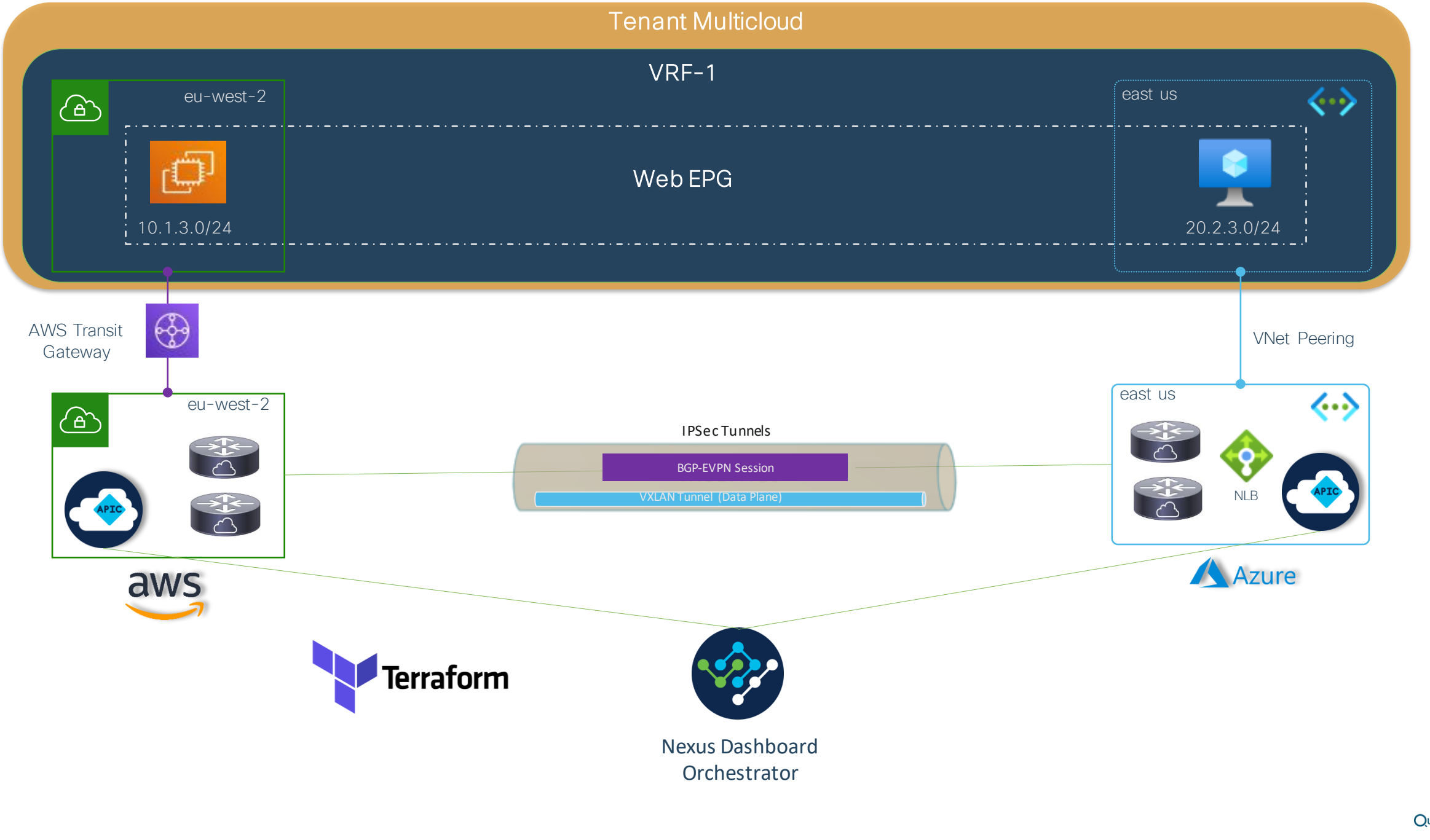


Configure the network **once**, deploy, monitor and secure **anywhere**

Quint@s Quinze

Demo Multicloud

Terraform e Nexus Dashboard



Quint@s Quinze

Dúvidas?

Review the content and pre-register to the **Nexus Dashboard Test Drive**

YouTube /CiscoDataCenterMadeEasy

cisco dCloud

Take an official Cisco ACI Training

Cisco Learning Network

DCACI
Implementing Cisco ACI

DCACIA
Implementing Cisco ACI Advanced

Get Certified on ACI and CCNP DC*

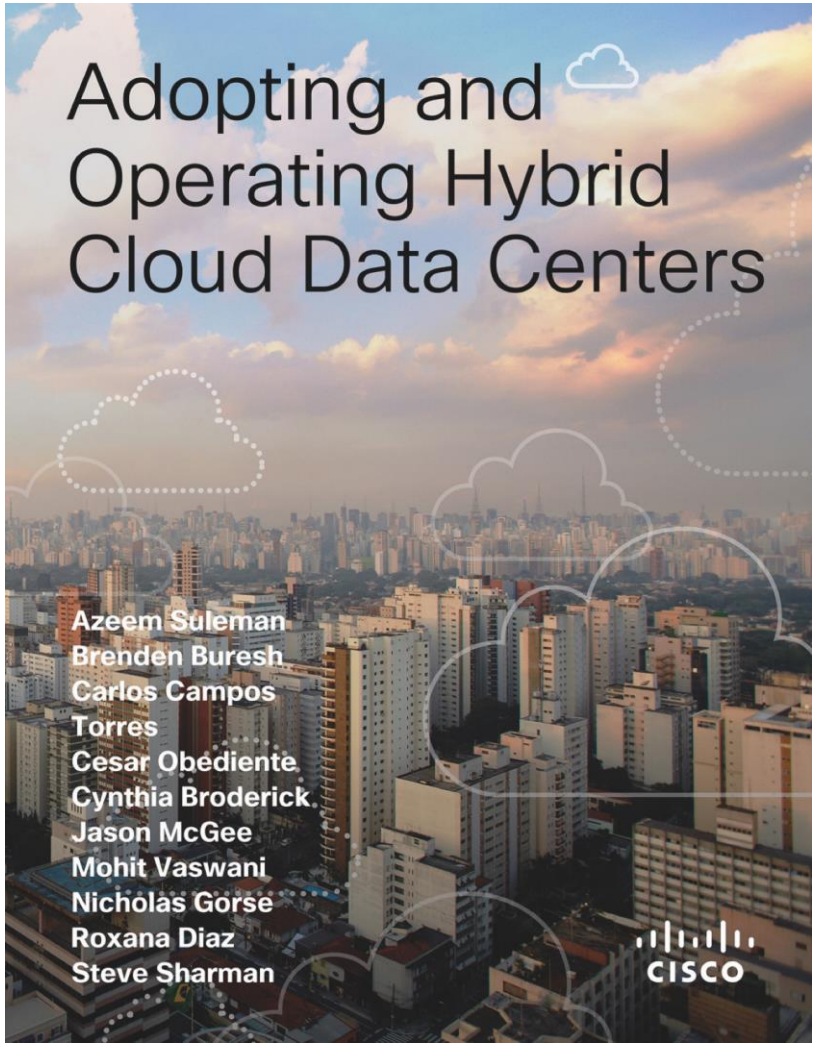
Cisco Certified CCNP Data Center · Cisco Certified Specialist

300-620 DCACI Exam
Implementing Cisco ACI

Cisco Certified Specialist

600-660 DCACIA
Implementing Cisco ACI Advanced

* CCNP through ACI Specialization requires passing both 350-601 DCCOR +300-620 DCACI



eBook: https://www.cisco.com/c/dam/en/us/products/se/2020/10/Collateral/data-center-ebook.pdf

Quint@s Quinze

Muito Obrigado!